VioStor NVR

Network Video Recorder

User Manual (Version: 3.1.0)

FOREWORD

Thank you for choosing QNAP products! This user manual provides detailed instructions of using the product. Please read carefully and start to enjoy the powerful functions of the product!

NOTE

- All features, functionality, and other product specifications are subject to change without prior notice or obligation.
- All brands and products names referred to are trademarks of their respective holders.

LIMITED WARRANTY

In no event shall the liability of QNAP Systems, Inc. (QNAP) exceed the price paid for the product from direct, indirect, special, incidental, or consequential software, or its documentation. QNAP makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. QNAP reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity.

CAUTION

1. Back up your system periodically to avoid any potential data loss. QNAP disclaims any responsibility of all sorts of data loss or recovery.
2. Should you return any components of the product package for refund or maintenance, make sure they are carefully packed for shipping. Any form of damages due to improper packaging will not be compensated.

Important Notice

- Reading instructions
  Please read the safety warnings and user manual carefully before using this product.
- Power supply
  This product can only be used with the power supply provided by the manufacturer.
- Service
  Please contact qualified technicians for any technical enquires. Do not repair this product by yourself to avoid any voltage danger and other risks caused by opening this product cover.
- Warning
  To avoid fire or electric shock, do not use this product in rain or humid environment. Do not place any objects on this product.

Table of Contents

Safety Warning

1. This product can operate normally in the temperature of 0ºC~40ºC and relative humidity of 0%~90%. Please make sure the environment is well-ventilated.
2. The power cord and devices connected to this product must provide correct supply voltage.
3. Do not place this product in direct sunlight or near chemicals. Make sure the temperature and humidity of the environment are in optimized level.
4. Unplug the power cord and all connected cables before cleaning. Wipe this product with a wet towel. Do not use chemical or aerosol to clean this product.
5. Do not place any objects on this product for the server's normal operation and to avoid overheat.
6. Use the flat head screws in the product package to lock the hard disks in this product when installing hard disks for proper operation.
7. Do not place this product near any liquid.
8. Do not place this product on any uneven surface to avoid falling off and damage.
9. Make sure the voltage is correct in your location when using this product. If you are not sure about the voltage, please contact the distributor or the local power supply company.
10. Do not place any object on the power cord.
11. Do not attempt to repair this product in any occasions. Improper disassembly of the product may expose you to electric shock or other risks. For any enquiries, please contact the distributor.
12. The chassis models should only be installed in the server room and maintained by the authorized server manager or IT administrator. The server room is locked by key or keycard access and only certified staff is allowed to enter the server room.

CAUTION

- RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.
- DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.

Chapter 1. Introduction

1.1 Overview

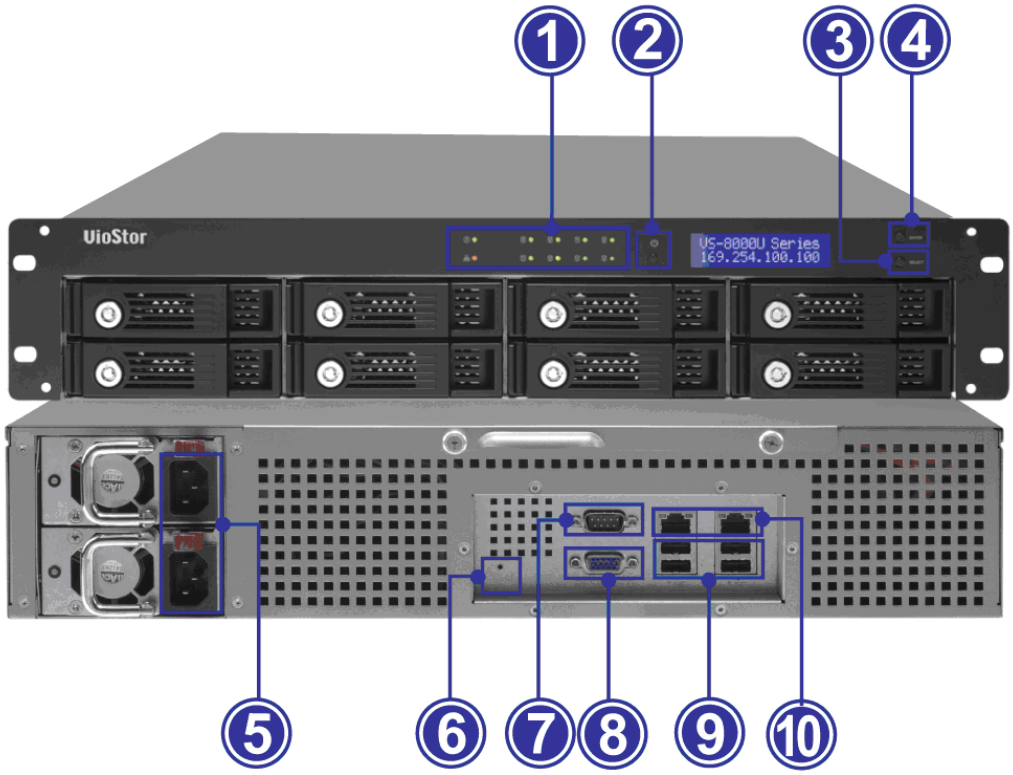
QNAP VioStor (hereafter referred to as NVR or VioStor) is the high performance 1U chassis network surveillance system featuring Linux-embedded OS and powerful surveillance features. It supports unique multi-server monitoring for up to 120-channel monitoring from multiple QNAP NVR servers simultaneously. Moreover, the NVR supports over 300 network camera models from AXIS, ACTi, Arecont Vision, Canon, D-Link, EDIMAX, ELMO, EtroVision, GANZ, iPUX, IQeye, LevelOne, MOBOTIX, Messoa, Panasonic BB/ BL/ i-Pro, SANYO, SONY, TOSHIBA, TRENDnet, VIVOTEK, and Y-CAM.

The NVR is a complete network surveillance solution which provides recording, real-time monitoring, and remote data access. It supports recording in H.264, MPEG-4, MxPEG, and MJPEG video compression. Besides, the NVR supports diversified recording features, e.g. schedule recording, alarm recording, alarm recording schedule, etc. In real-time monitoring, you can select to view the channels (IP cameras) with different display modes or drag and drop to change the display order of the channels flexibly. The NVR also intelligent video analytics, including motion detection, missing object, foreign object, out of focus, and camera occlusion. It offer smart control of PTZ cameras, instant alarm alert, digital zoom, data search by date and time, timeline, and event. All the functions can be configured by the IE web browser.

* MxPEG video compression is not supported by VS-201, VS-101, NVR-104.

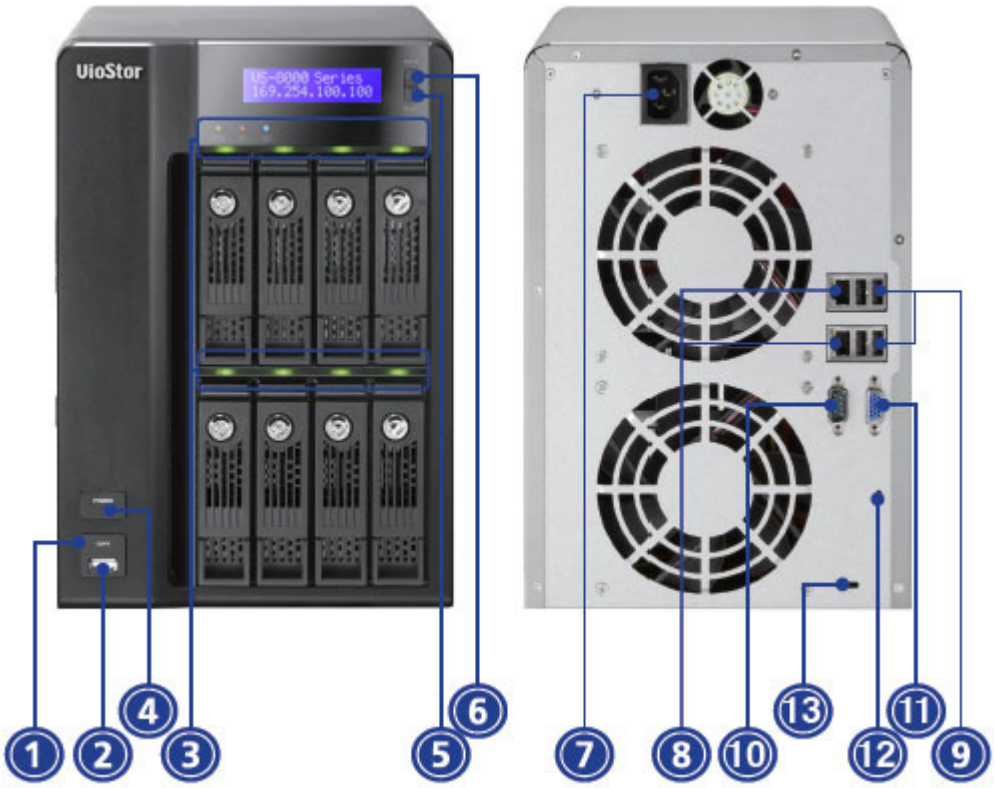
1.2 Hardware Illustration

1.2.1 VS-8040U-RP/ VS-8032U-RP/ VS-8024U-RP



1. LED indicators: Status, LAN, USB, HDD1-8
2. Power button
3. Select button
4. Enter button
5. Power connector
6. Password & network settings reset button
7. RS-232
8. VGA
9. USB 2.0 x 4
10. Giga LAN x 2

1.2.2 VS-8040/ VS-8032/ VS-8024

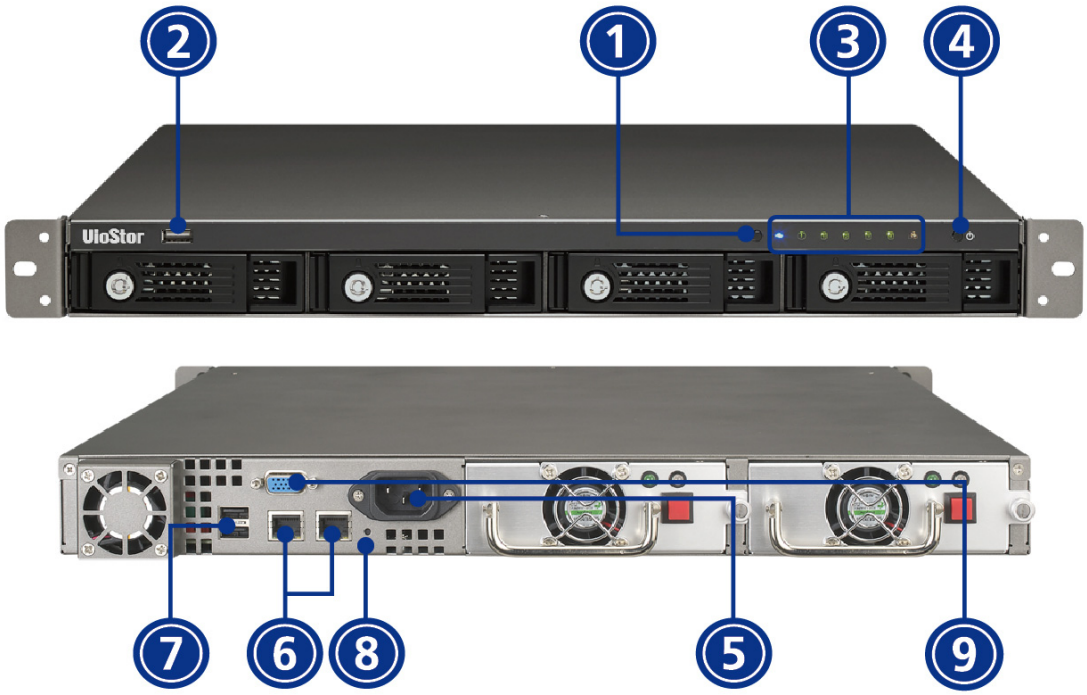


1. One touch auto video backup button
2. USB 2.0
3. LED indicators: Status, LAN, USB, HDD1-8
4. Power button
5. Select button
6. Enter button
7. Power connector
8. Giga LAN x 2
9. USB 2.0 x 4
10. RS-232
11. VGA
12. Password & network settings reset button
13. K-lock security slot

1.2.3 VS-5012/ VS-5020

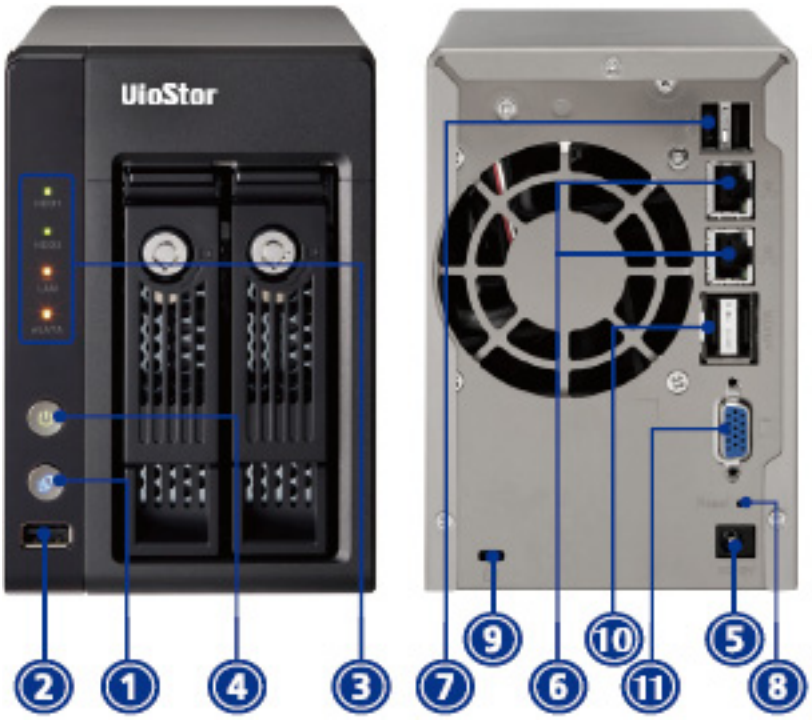
1. One touch auto video backup button
2. USB 2.0
3. LED indicators: USB, Status, HDD1~HDD5, LAN
4. Power button
5. Select button
6. Enter button
7. Power connector
8. Giga LAN x 2
9. USB 2.0 x 4
10. eSATA connector
11. (Reserved)
12. RS-232 port
13. Password & network settings reset button
14. K-lock security slot

1.2.4 VS-4016U-RP



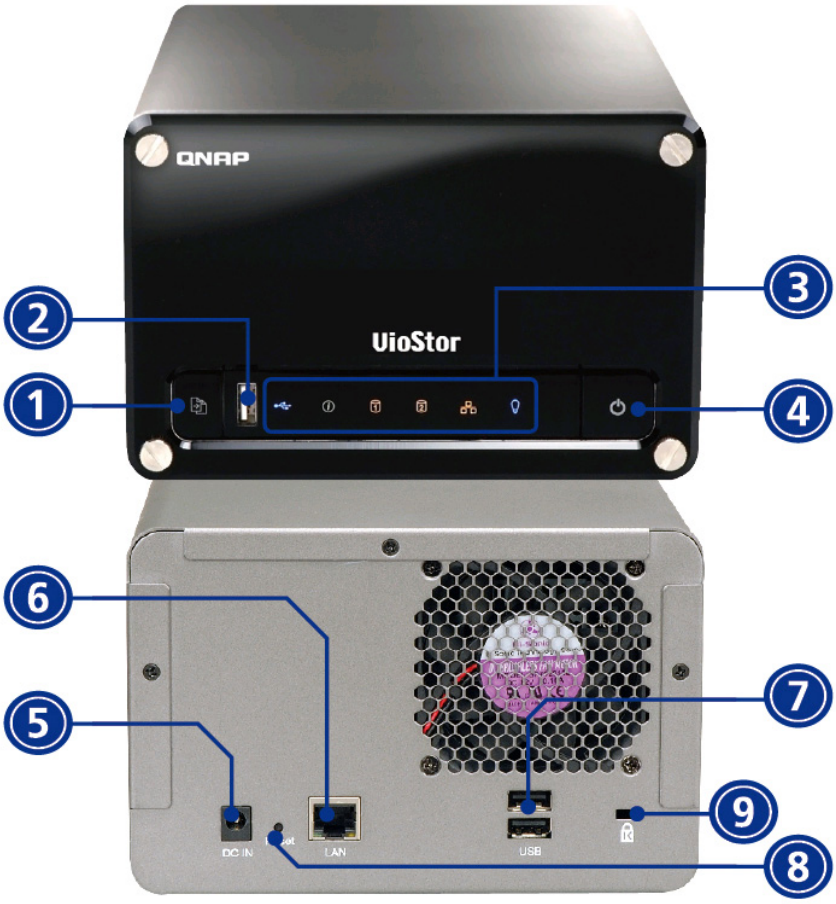
1. One touch auto video backup button
2. USB 2.0
3. LED indicators: USB, Status, HDD1~HDD4, LAN
4. Power button
5. Power connector
6. Giga LAN x 2
7. USB 2.0 x 2
8. Password & network settings reset button
9. VGA (reserved)

1.2.5 VS-2008/ VS-2012



1. One touch auto video backup button
2. USB 2.0
3. LED Indicators: HDD1, HDD2, LAN & eSATA
4. Power button
5. Power Connector
6. Giga LAN x 2
7. USB 2.0 x 2
8. Password & Network Settings Reset Button
9. K-Lock Security Slot
10. eSATA x 2 (Reserved)
11. VGA (Reserved)

1.2.6 VS-201



1. Backup Button (One touch auto video backup)
2. USB 2.0
3. LED Indicators: USB, Status, HDD1, HDD2, LAN, and Power
4. Power Button
5. Power Connector
6. Giga LAN
7. USB 2.0 x 2
8. Configuration Reset Switch (Password & network settings)
9. K-Lock Security Slot

1.2.7 NVR-104

1. One Touch Auto Video Backup Button
2. USB 2.0
3. LED Indicators
4. Power Button
5. USB 2.0 x 2
6. eSATA Port
7. Giga LAN
8. Password & Network Settings Reset Button
9. Power Connector
10. K-lock Security Slot

1.2.8 VS-101

1. One Touch Auto Video Backup Button
2. USB 2.0
3. LED Indicators
4. Power Button
5. Power Connector
6. Giga LAN
7. USB 2.0 x 2
8. Password & Network Settings Reset Button
9. K-lock Security Slot
10. eSATA Port

Chapter 2. Install the VioStor

For the information of the hardware installation, please refer to the "Quick Installation Guide" in the product package.

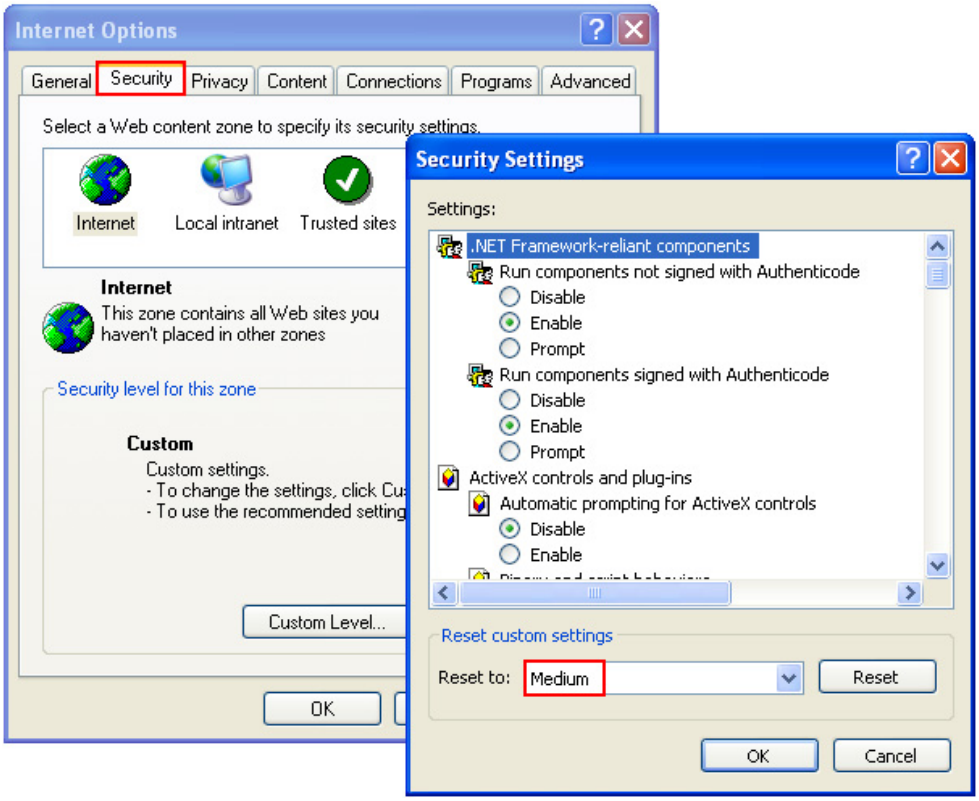
2.1 Personal Computer Requirements

For better system performance, your computer should at least fulfill the following requirements:

No. of Channels	Format	CPU	Others
4	Motion JPEG	Intel® Pentium 4 CPU, 2.0 GHz or above	• Operation system: Microsoft® Windows® XP/ Vista (32-bit) • Memory: 1 GB or above • Network port: 100Mbps Ethernet port or above • Web browser: Microsoft® Internet Explorer 6.0 or above • CD-ROM drive • Recommended resolution: 1024 x 768 pixels or above
	MPEG-4/ MxPEG/ H.264	Dual core CPU, 2.0 GHz or above	
8	Motion JPEG	Intel® Pentium 4 CPU, 2.2 GHz or above	
	MPEG-4/ MxPEG/ H.264	Dual core CPU, 2.2 GHz or above	
12	Motion JPEG	Intel® Pentium 4 CPU, 2.4 GHz or above	
	MPEG-4/ MxPEG/ H.264	Dual core CPU, 2.4 GHz or above	
16	Motion JPEG	Intel® Pentium 4 CPU, 2.6 GHz or above	
	MPEG-4/ MxPEG/ H.264	Dual core CPU, 2.6 GHz or above	
20	Motion JPEG	Intel® Pentium 4 CPU, 2.8 GHz or above	
	MPEG-4/ MxPEG/ H.264	Dual core CPU, 2.8 GHz or above	
40	Motion JPEG	Dual core CPU, 2.4 GHz or above	
	MPEG-4/ MxPEG/ H.264	Dual core CPU, 2.4 GHz or above	

Security Settings of the Web Browser

Please make sure the security level of the IE browser in Internet Options is set to Medium or lower.



2.2 Hard Disk Compatibility List

This product works with 3.5” SATA hard disk drives from major hard disk brands. For the HDD compatibility list, please visit http://www.qnapsecurity.com/.

QNAP disclaims any responsibility for product damage/ malfunction or data loss/ recovery due to misuse or improper installation of hard disks in any occasions for any reasons.

2.3 Network Camera Compatibility List

For the information of supported camera models, please visit QNAP Security website http://www.qnapsecurity.com/.

2.4 Check System Status

LED Display & System Status Overview

LED	Colour	LED Status	Description
USB	**Blue**	Flashes blue every 0.5 sec	1) A USB device is detected 2) A USB device is being removed from the NVR 3) The USB device connected to the front USB port of the NVR is being accessed 4) The NVR data is being copied to the external USB device
		Blue	The USB device connected to the front USB port of the NVR is ready
		Off	The NVR has finished copying the data to the USB device connected to the front USB port*
eSATA†	**Orange**	Flashes	The eSATA device is being accessed
System Status	**Red/ Green**	Flashes green and red alternately every 0.5 sec	1) The hard drive on the NVR is being formatted 2) The NVR is being initialised 3) The system firmware is being updated 4) RAID rebuilding is in process 5) Online RAID Capacity Expansion is in process 6) Online RAID Level Migration is in process

		Red	1) The hard drive is invalid 2) The disk volume has reached its full capacity 3) The disk volume is going to be full 4) The system fan is out of function* 5) An error occurs when accessing (read/write) the disk data 6) A bad sector is detected on the hard drive 7) The NVR is in degraded read-only mode (2 member drives fail in a RAID 5 or RAID 6 configuration, the disk data can still be read)# 8) (Hardware self-test error)
System Status	**Red/ Green**	Flashes red every 0.5 sec	The NVR is in degraded mode (one member drive fails in RAID 1, RAID 5 or RAID 6 configuration)*
		Flashes green every 0.5 sec	1) The NVR is starting up 2) The NVR is not configured 3) The hard drive is not formatted
		Green	The NVR is ready
		Off	All the hard drives on the NVR are in standby mode
HDD	**Red/ Green**	Flashes red	The hard drive data is being accessed and a read/ write error occurs during the process
		Red	A hard drive read/ write error occurs
		Flashes green	The hard drive data is being accessed
		Green	The hard drive can be accessed
LAN	**Orange**	Orange	The NVR is connected to the network
		Flashes orange	The NVR is being accessed from the network

* Not applicable to 1-bay models

† The eSATA port is available on certain models only. Please refer to the product specifications for more information.

4-bay models or above only

Beep Alarm (beep alarm can be disabled in "System Tools" > "Hardware Settings")

Beep sound	No. of Times	Description
Short beep (0.5 sec)	1	1) The NVR is starting up 2) The NVR is being shut down (software shutdown) 3) The user presses the reset button to reset the NVR 4) The system firmware has been updated
Short beep (0.5 sec)	3	The user tries to copy the NVR data to the external storage device from the front USB port, but the data cannot be copied.
Short beep (0.5 sec), long beep (1.5 sec)	3, every 5 min	The system fan is out of function*
Long beep (1.5 sec)	2	1) The disk volume is going to be full 2) The disk volume has reached its full capacity 3) The hard drives on the NVR are in degraded mode 4) The user starts the HDD rebuilding process
	1	1) The NVR is turned off by force shutdown (hardware shutdown) 2) The NVR has been turned on successfully and is ready

* Not applicable to 1-bay models

2.5 System Configuration

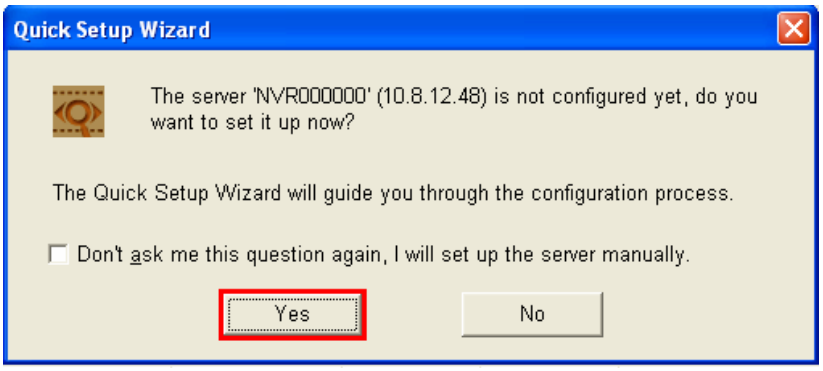
Install the Finder

1. Execute the product CD, the following menu is shown. Click "Install Finder".

2. Follow the instructions to install the Finder. If you are using Windows XP SP2 or above, the following screen will be shown. Click "Unblock".

3. The Finder detects the VioStor in the network and prompts you to perform quick setup. Click "Yes" to continue.

Note: If the VioStor is not found, click "Refresh" to try again.



4. You must enter the administrator name and password to perform quick setup.

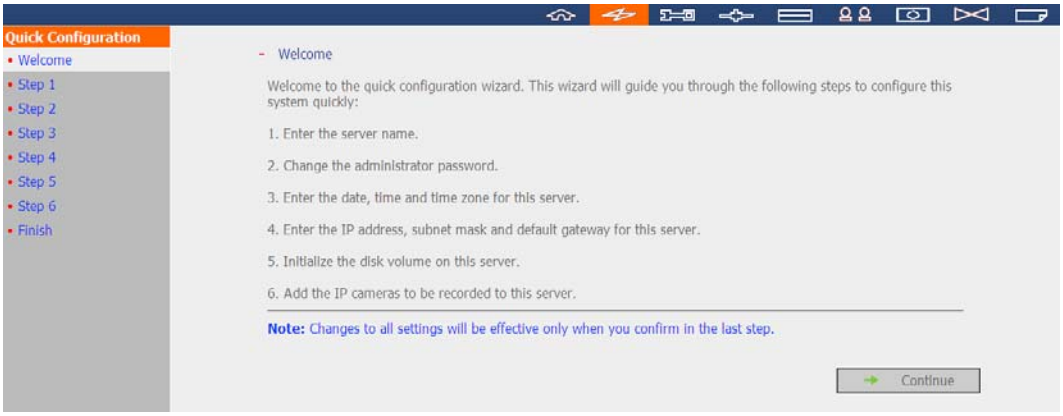
The default administrator name and password are as below:

Use name: **admin***
Password: **admin**

*If you are using VS-201/ VS-101/ NVR-104, the login name is 'administrator' and the login password is 'admin'.

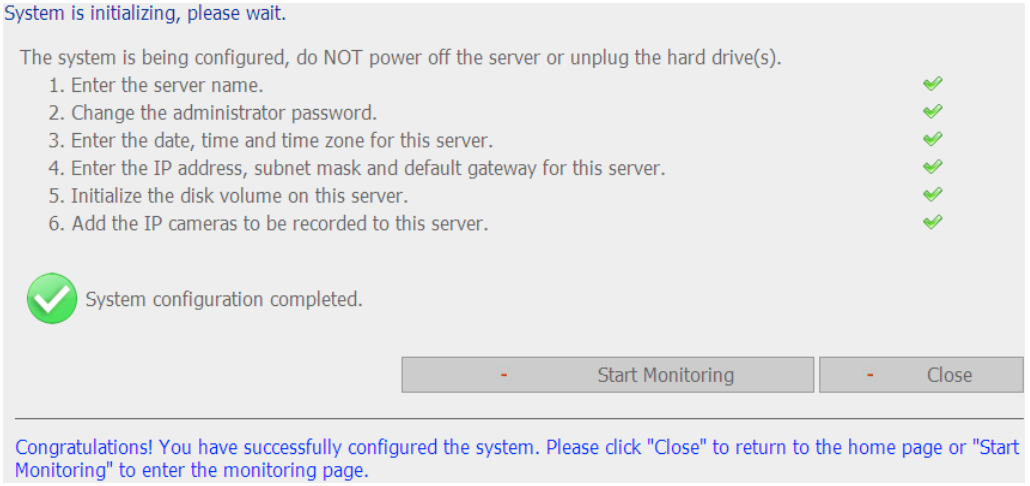
Note: Please make sure all the network cameras are configured and connected to the network.

5. The quick configuration page will be shown. Click "Continue" and follow the instructions to finish the configuration. For further information, please refer to Chapter 5.1.

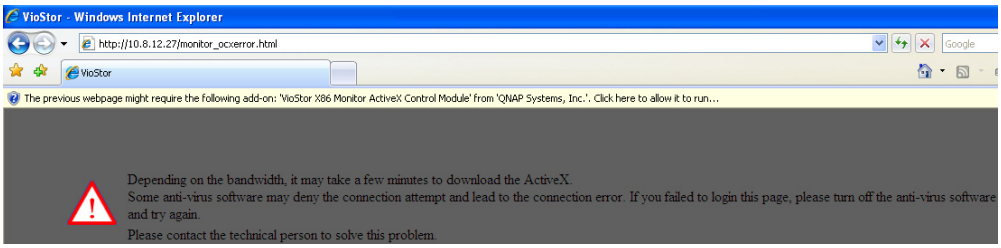


6. Click “Start installation” to execute the quick configuration.

7. The quick configuration is completed and you can start to use the VioStor. Click “Start Monitoring” to view the live video from the cameras or click “Close” to return to the system administration home page.



8. The first time you connect to the server, please install the ActiveX. Follow the instructions to install the ActiveX.



When the live video is displayed and the recording indicator is shown, you have successfully installed the VioStor.

Chapter 3. Start to Use the VioStor

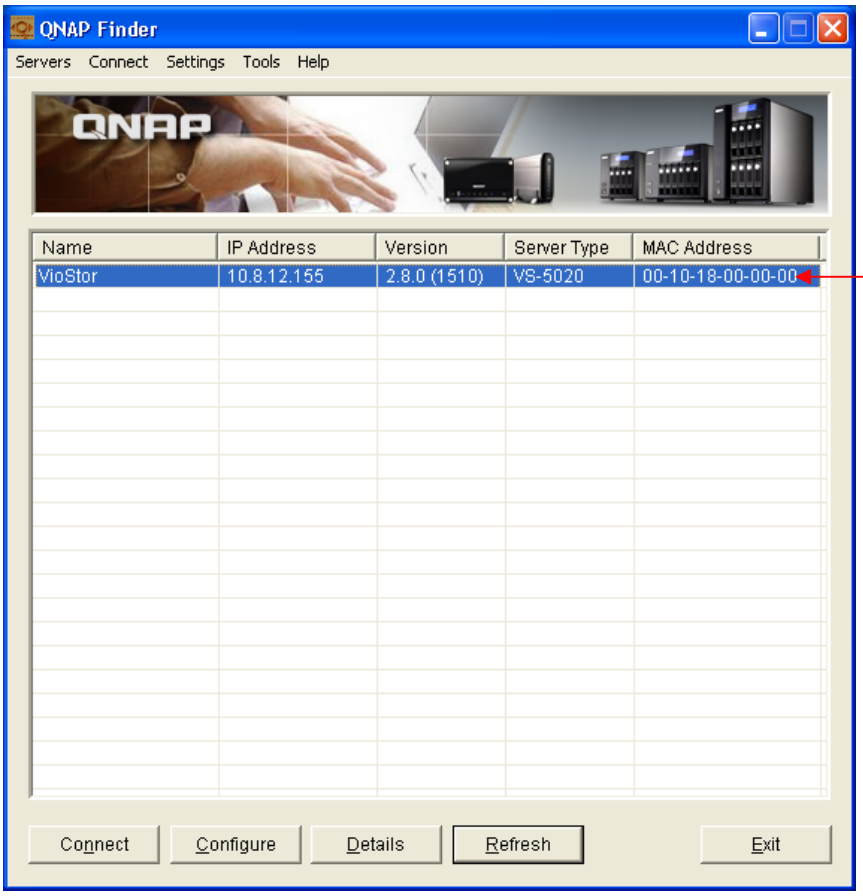
When you have installed the VioStor and other hardware, and connected it to the network, you can use the browser in your PC to connect to the VioStor. It is recommended to use Microsoft Internet Explorer 6.0 for browsing.

Important Notice:
Before you start to use the VioStor, you must install the hard disks in the VioStor, finish disk volume configuration and format the hard disk(s). Otherwise, the system may not function properly.

3.1 Connect to the VioStor

Follow the steps below to connect to the VioStor monitoring page:

1. Open an IE browser and enter the IP address of the VioStor or run Finder. When the following screen is shown, double click the name of the VioStor.



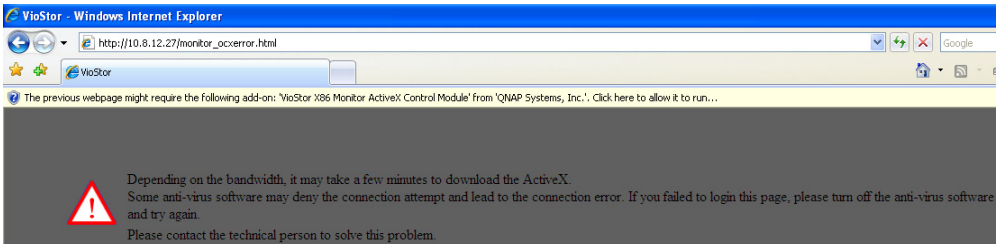
Double click VioStor name to login the server

2. Enter the user name and password to login the VioStor.

Default User name: **admin***
Default Password: **admin**

* If you are using VS-201/ VS-101/ NVR-104, the login name is 'administrator' and the login password is 'admin'.

3. To view the live video, you must install the ActiveX control. Follow the instructions to install it.

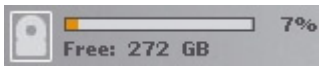


3.2 Monitoring Page

When you have successfully logged in the VioStor, the monitoring page is shown. Select the display language. You can start to configure the system settings and use the monitoring and recording functions of the server.

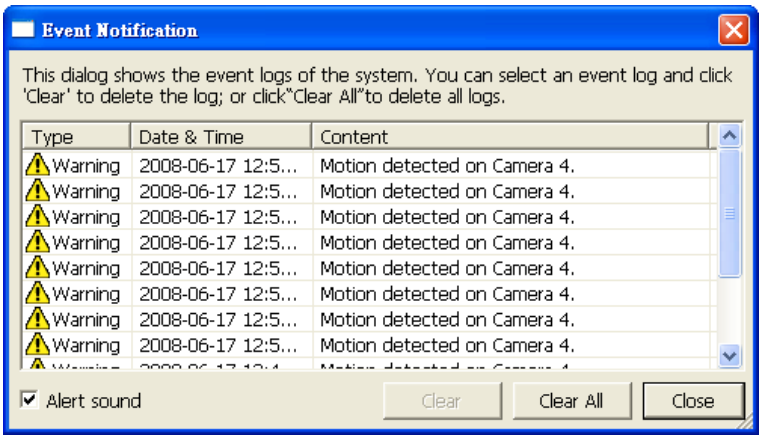
Icon	Description
	Multi displays Supports multi-display mode. (This function can only be used when the computer or the host is connected to multiple monitors.)
	Multi-server monitoring: Up to 120 channels from different NVR servers can be added for monitoring.
	Select language: Select the display language.
	E-map: Displays the location of the camera. The e-map can be changed in system configuration page.

	**System configuration:** Login the system administration page.
	**Monitor settings:** Configure the advanced settings of monitoring page. You can configure the source of video/ audio stream, event notification, and snapshot folder.
	**Playback:** Enter the recording playback page. The administrator can grant access right to the users.
	**Help:** View the system online help.
	**Logout:** Logout the VioStor.
	**Snapshot:** Take a snapshot on the selected camera. When the picture is shown, right click the picture to save it to the computer.
	**Manual recording:** Enable or disable manual recording on the selected camera. The administrator can enable or disable this option in the system configuration page.
	**Audio (optional):** Turn on/ off the audio support for the monitoring page.
	**Login network camera homepage:** Select a camera and click this button to go to the homepage of the selected camera.
	**Event notification:** When the alarm recording is enabled and an event is detected, this icon is shown. Click this icon to view the alert details.
	**Digital zoom:** Select a camera and click this button to enable the digital zoom function of the camera. (You can also right click the monitoring channel to enable this function.) Press and hold the left mouse button to zoom in or press and hold the right mouse button to zoom out. You can press the left mouse button to drag the viewing angle of the camera.

	You can also use the mouse wheel or the PTZ control panel to use the digital zoom function.
	**Focus control:** Focus control of the PTZ camera.
	**Select PTZ camera preset positions:** You can view different preset positions of the camera by clicking the number buttons. To configure the preset positions of the camera, please refer to the user manual of the camera.
	**Recording storage status:** Displays the storage percentage and the free space.

Note:

1. Starting and stopping manual recording will not affect the scheduled or alarm recording.
2. The default path for storing snapshots is the "Snapshot" folder under My Documents in your computer.
3. If the snapshot time is inconsistent with the actual time that the snapshot is taken, it is caused by the network environment but not a system error.
4. Click the event notification icon to view the event details, enable or disable the alert sound or clear the event logs.



5. When the digital zoom function is enabled on multiple cameras, the zooming function will be affected if your computer performance is not high enough.
6. Right click the monitoring channel on the live view page. The following functions are available depending on the camera model.
   a. Connect to camera homepage.
   b. Camera setting: Enter the camera configuration page.
   c. PTZ: Pan/ Tilt/ Zoom camera control.
   d. Preset: Select PTZ camera preset positions.

e. Enable live tracking: Available on Panasonic NS202(A) camera.
f. Disable live tracking: Available on Panasonic NS202(A) camera.
g. Auto cruising: This feature is used to configure the PTZ cameras to cruise according to the preset positions and the staying time set for each preset position.
h. Digital zoom: Enable/ disable digital zoom.
i. Keep aspect ratio.

3.2.1 Live Video Window

If the camera is properly configured, you can see the current video from the remote network camera.
If your camera supports pan and tilt functions, you can click on the video window directly to adjust the viewing angle. If the camera supports zooming, you can use a wheel mouse to adjust the zooming distance by scrolling the wheel. Please refer to the user manual of your camera for further information.

When you enable digital zoom, you can right click the camera and control the PTZ function. You can press and hold the left mouse button to zoom in or press and hold the right mouse button to zoom out, or press the left mouse button to drag the viewing angle of the camera.

Camera Status

The camera status is indicated by the icons shown below:

Icon	Camera Status
	Scheduled or continuous recording is in process
	This camera supports audio function
	This camera supports PT function
	Manual recording is enabled
	The alarm input 1 of the camera is triggered and recording is in process
	The alarm input 2 of the camera is triggered and recording is in process
	The alarm input 3 of the camera is triggered and recording is in process
	Motion detection recording is in process
	Digital zoom is enabled

Connection Message

When the VioStor fails to display a camera, a message will be shown within the live video window. The following messages may be shown:

- Connecting

  If the network camera is located in remote network or Internet, it may take some time to establish connection to the camera.
- Disconnected

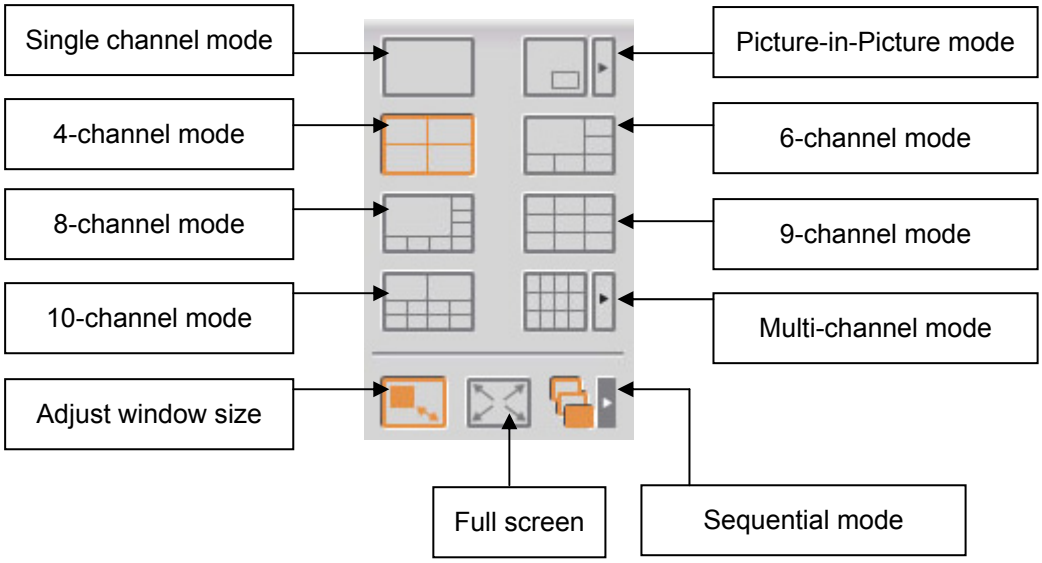
  The system cannot connect to the network camera. Please check the network connection of your computer and the availability of the network camera. If the camera is installed on the Internet, the port for the camera must be opened on your router or gateway.
- No Permission

  This message is shown when a user without access right to view this camera. Please logout the system and login as a user with the access right to the camera.
- Server Error

  Please check the camera settings or update camera's firmware to newer version. Contact the technical support if the problem is not fixed after checking.

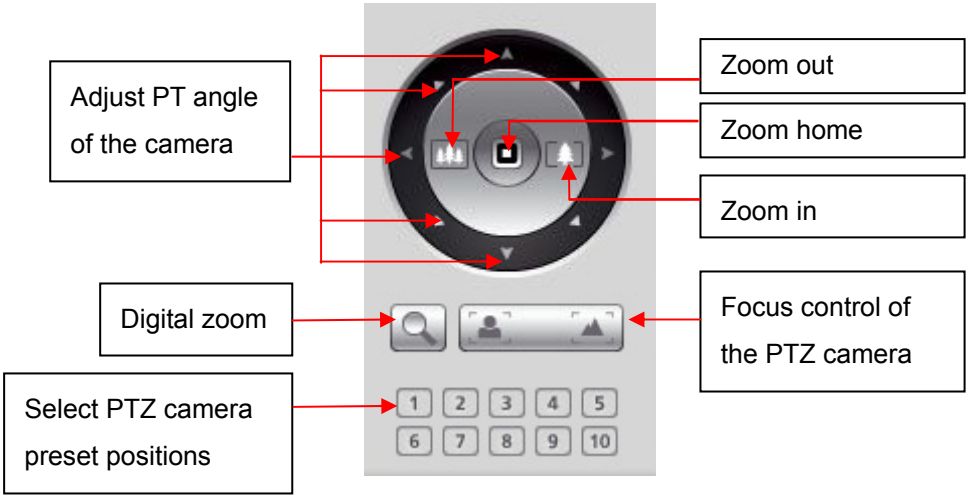
3.2.2 Display Mode

By changing the display mode, you can adjust the visual effects when viewing video of single or multiple cameras.



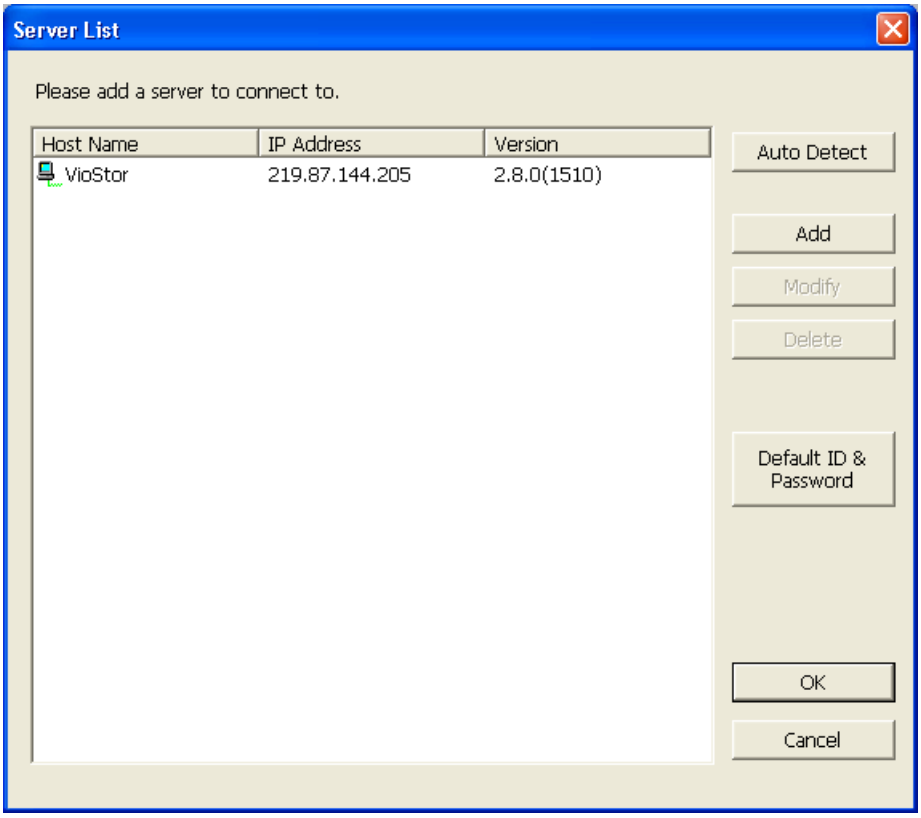
3.2.3 PTZ Camera Control Panel

PTZ stands for Pan/ Tilt/ Zoom camera control. You can do PTZ control on the selected camera. These functions are available depending on the camera model; please refer to the user manual of the camera. The digital zoom function cannot be used with the PTZ function at the same time.



3.2.4 Multi-server Monitoring

1. Click "Server List" on the live view page.



   a. Click "Auto Detect" to search for the QNAP NVR in the LAN and add the server to the server list.
   b. Click "Add" to add the QNAP NVR to the server list.

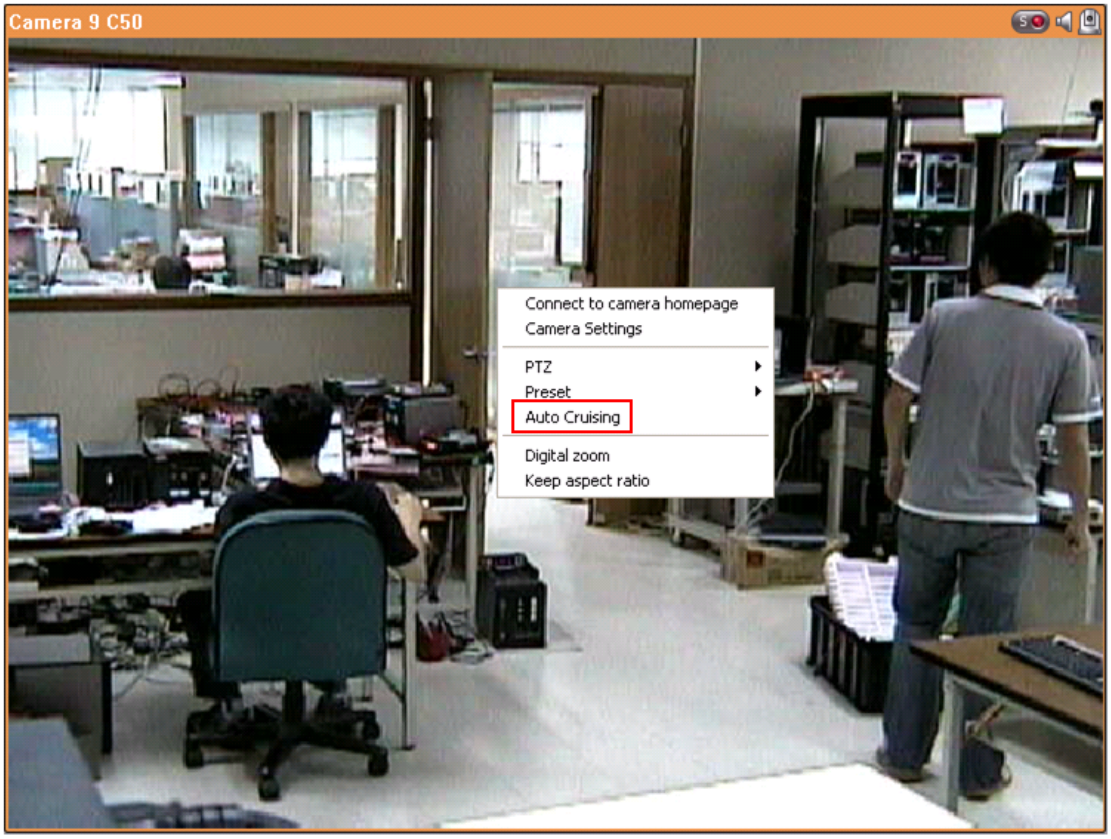
2. Up to 120 channels from different NVR servers can be added for monitoring.

3.2.5 Auto Cruising

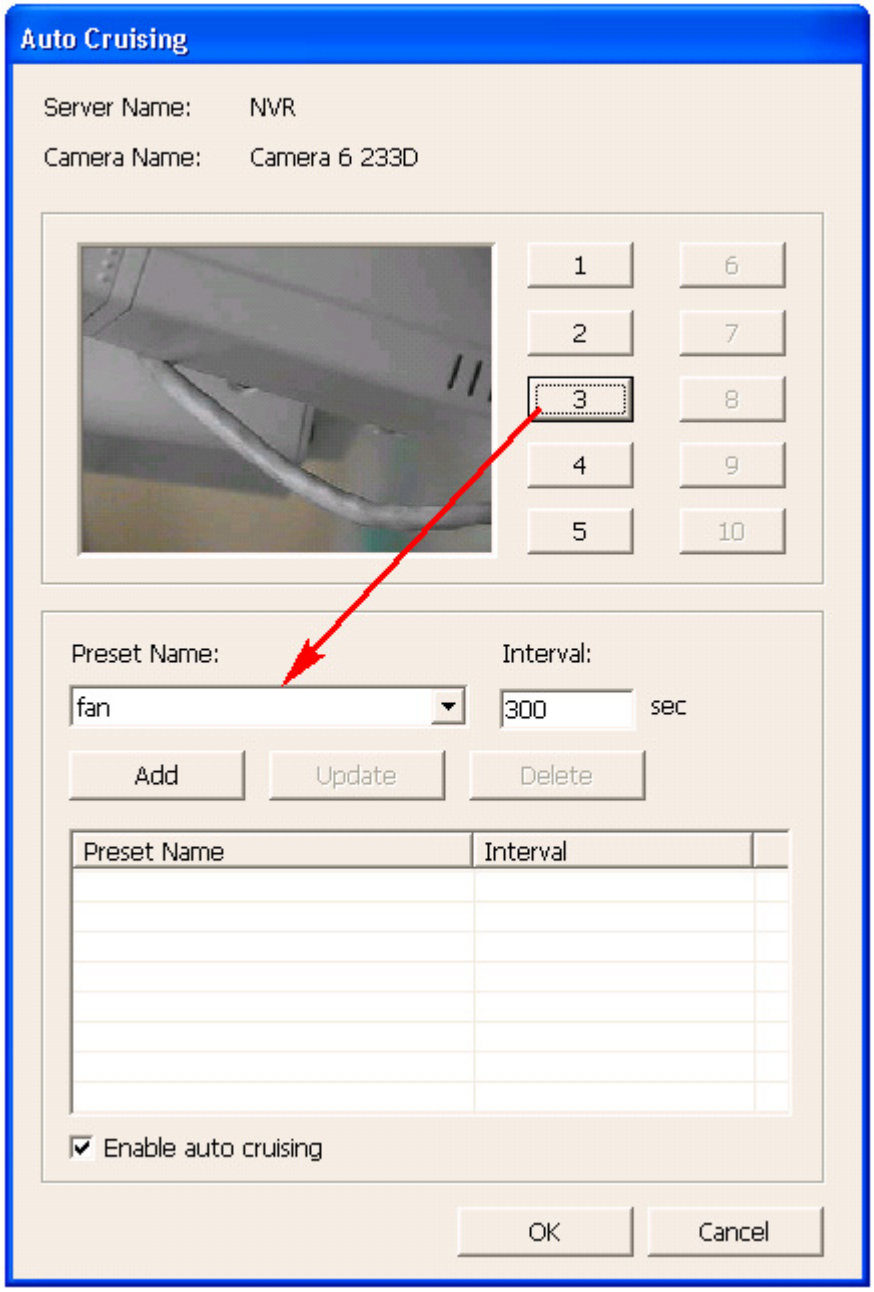
The auto cruising feature of the VioStor NVR is used to configure the PTZ cameras to cruise according to the preset positions and the staying time set for each preset position.

To use the auto cruising feature, follow the steps below.

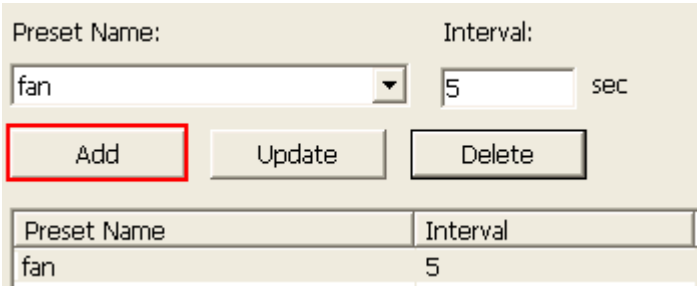
1. On the monitoring page of the VioStor NVR, click  to go to the configuration page of the PTZ camera.
2. Set the preset positions on the PTZ camera.
3. Return to the monitoring page of the VioStor NVR. Right click the display of the PTZ camera. Select "Auto Cruising".



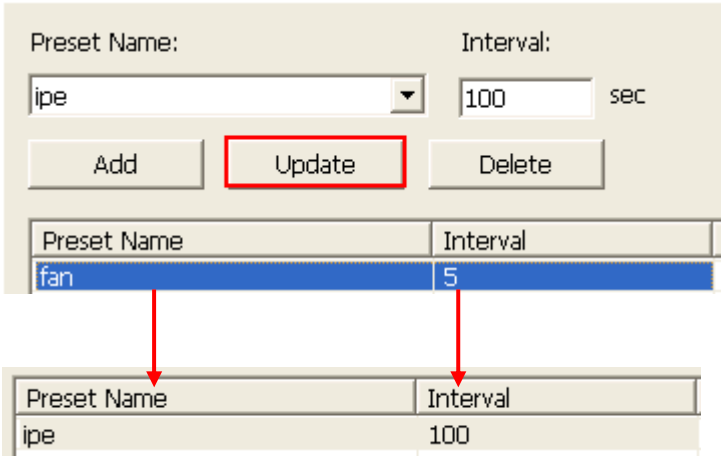
4. Click the number buttons to view the preset positions of the PTZ camera. When you click the button, the name of the corresponding preset position is shown on the "Preset Name" drop down menu.



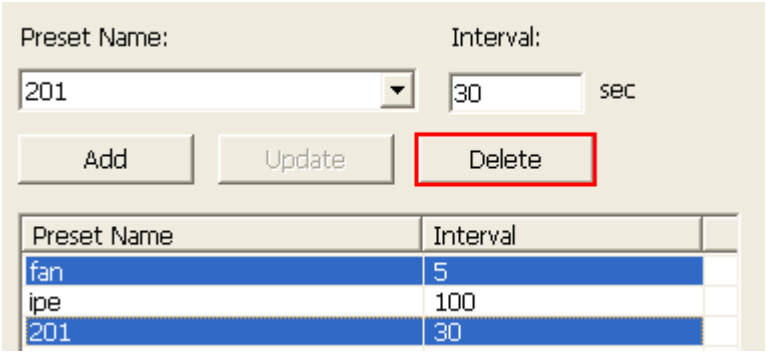
5. Add: To add a setting for auto cruising, select the "Preset Name" from the drop down menu and enter the staying time (interval, in seconds). Click "Add".



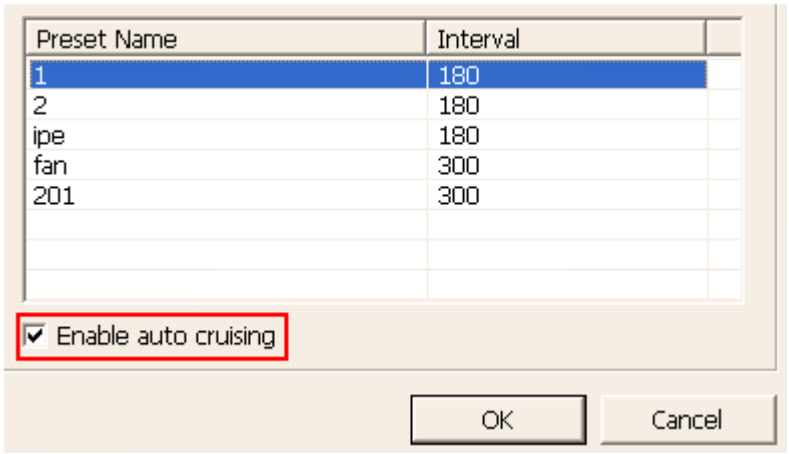
6. Update: To change a setting on the list, highlight the selection. Select another preset position from the drop down menu and/or change the staying time (interval). Click "Update".



7. Delete: To delete a setting, highlight a selection on the list and click "Delete". To delete more than one setting, press and hold the Ctrl key and click the settings. Then click "Delete".



8. After configuring the auto cruising settings, check the box "Enable auto cruising" and click "OK". The system will start auto cruising according to the settings.



Note:

1) The default staying time (interval) of the preset position is 5 seconds. You can enter 5-999 seconds for this setting.
2) The system supports up to 10 preset positions (the first 10) configured on the PTZ cameras. You can configure up to 20 settings for auto cruising on the NVR. In other words, the NVR supports maximum 10 selections on the drop down menu and 20 settings on the auto cruising list.

Chapter 4. Playback the Video Files

The VioStor provides an intuitive web interface to search and play recording files, no extra software installation is necessary. In addition, you can use network file services to access the recorded video files directly.

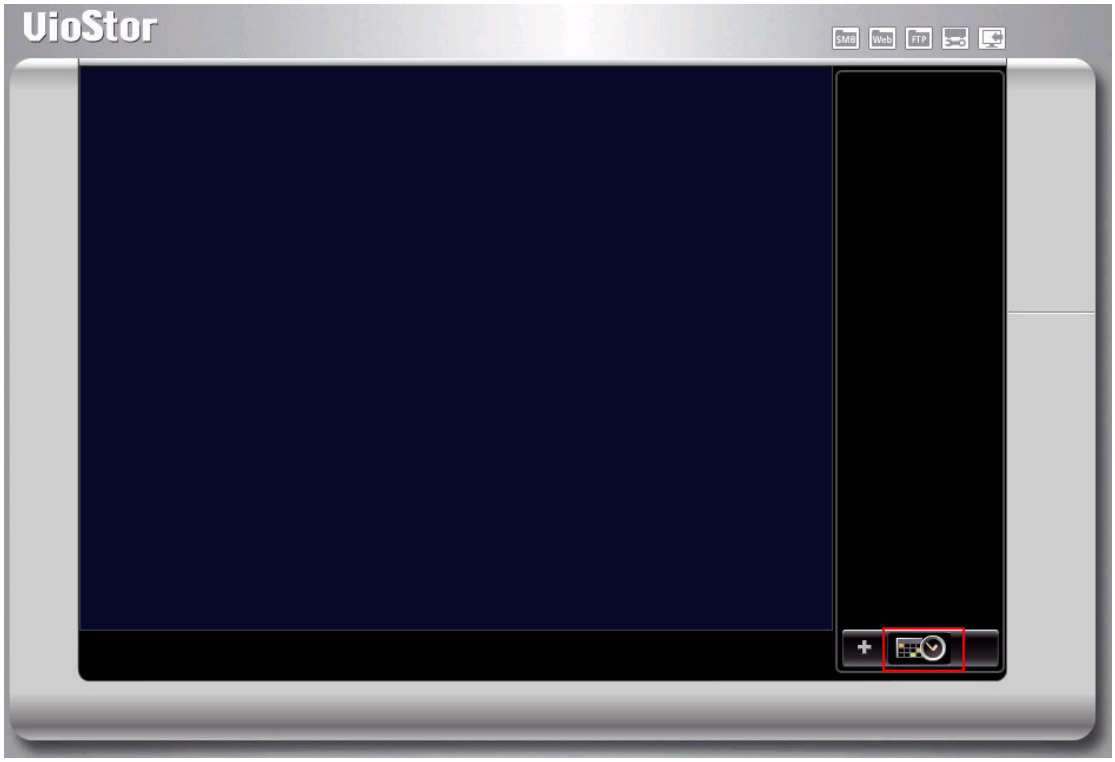
4.1 Use the Web Playback Interface (VioStor Player)

1. Click the playback button on the monitoring page.
2. VioStor Player will be shown. You can use this program to search and play the recording files on the NVR servers. To return to the monitoring page, click . To enter the system administration page, click .

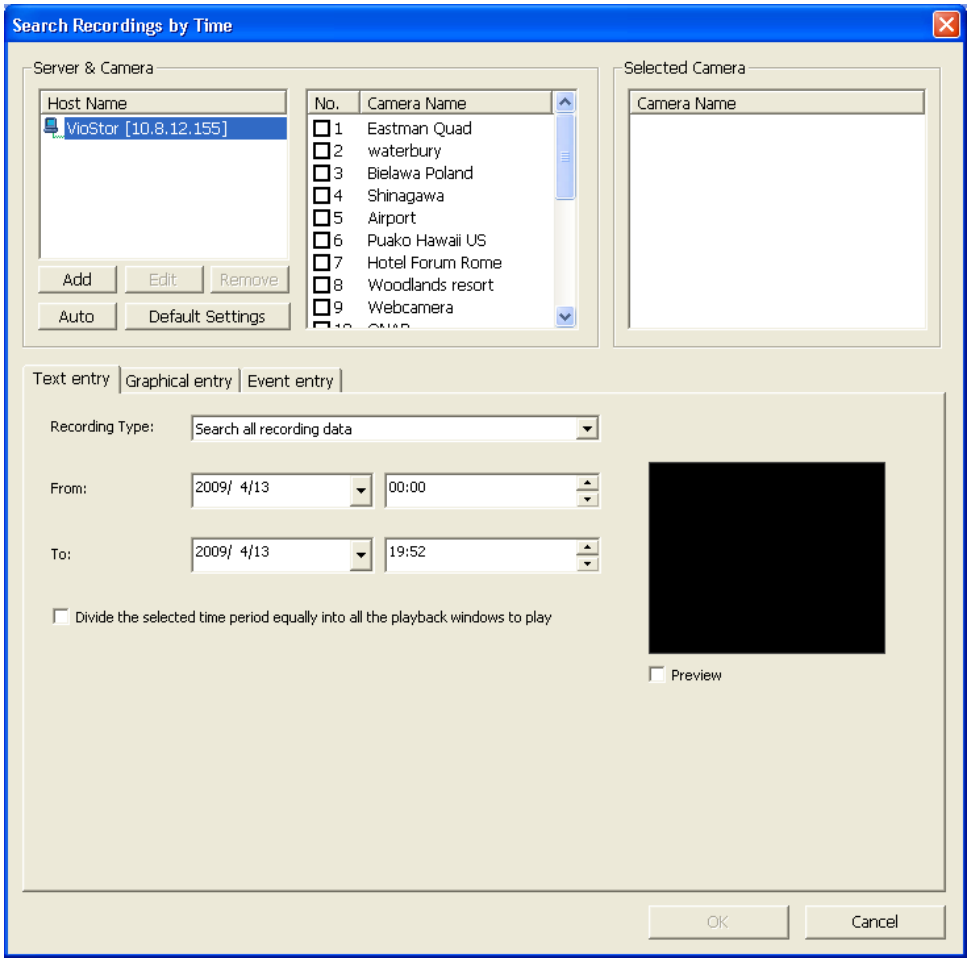
Note: If you do not have access authority of the cameras, you will not be able to get the recording file list and play the video recordings of the cameras. Please refer to Chapter 5.5 for access right configuration.

4.1.1 Connect to Server for Playback

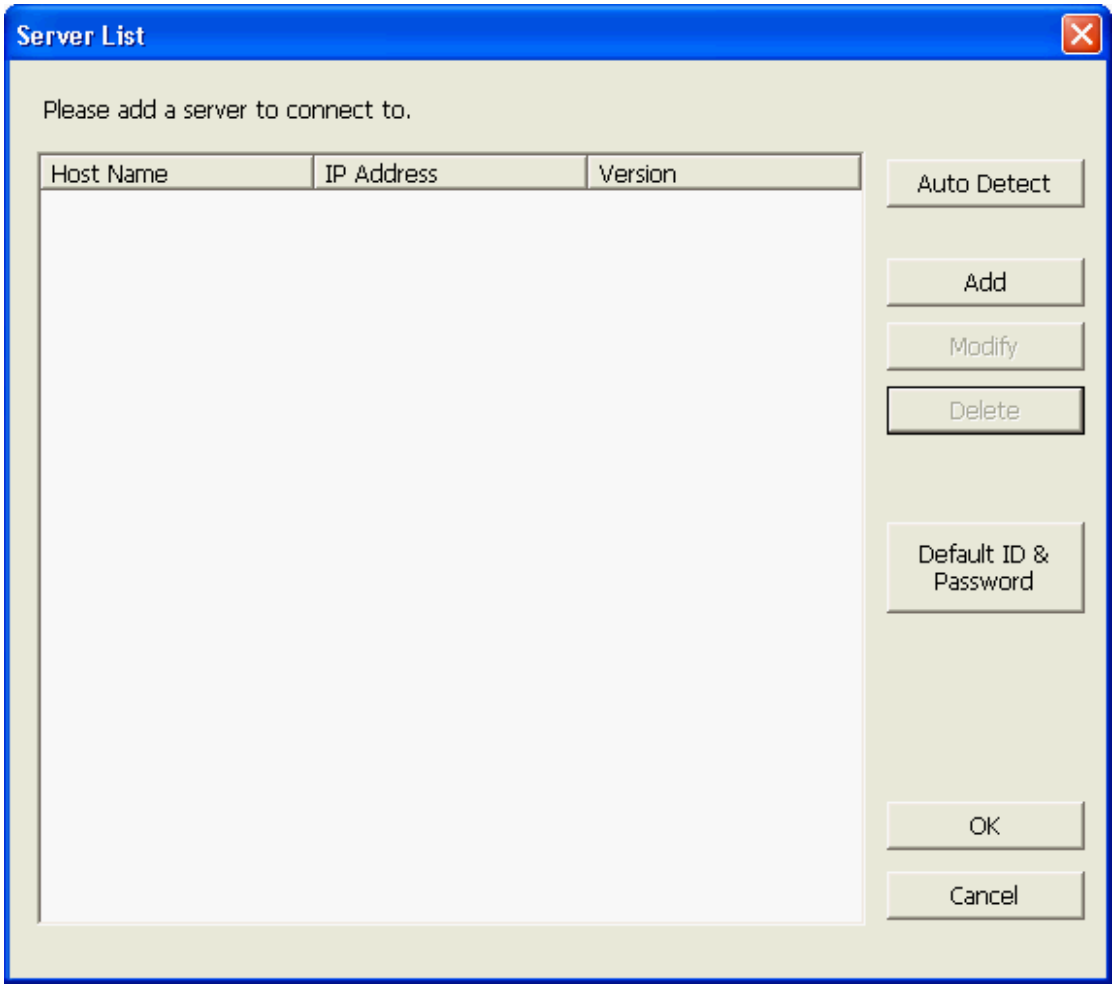
1. Click "Play by Time"  .



2. The following dialog will be shown.

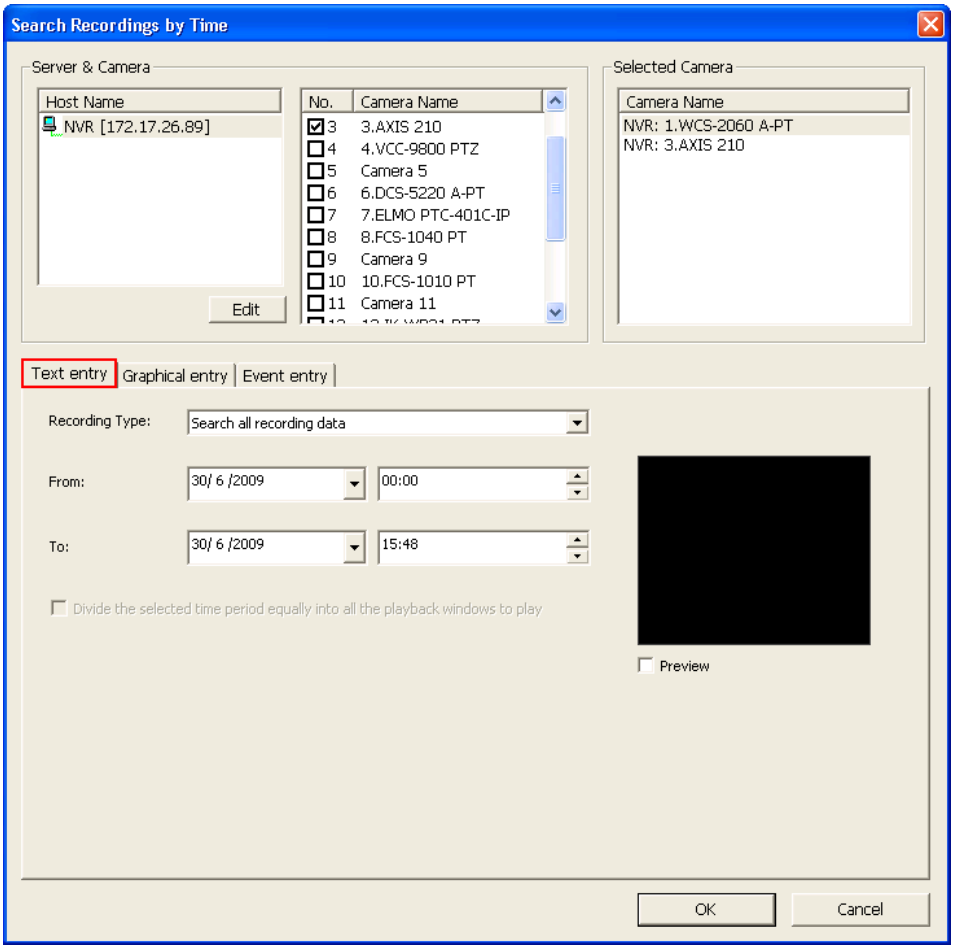


3. Configure servers:
   a. Add: Add a server.
   b. Modify: Modify a server.
   c. Remove: Remove a server.
   d. Auto: Auto-search servers.
   e. Default settings: Enter the default user name and password for all newly added servers.



4. Select the data search mode.
   - **Date and time search (Text entry)**
     i. Select the NVR server(s) and the IP camera(s)*.
     ii. Click the "Text entry" tab.
     iii. Select the recording type, the start and end time when the video is recorded.
     iv. Click "Preview" to preview the searched video.
     v. Click "OK".

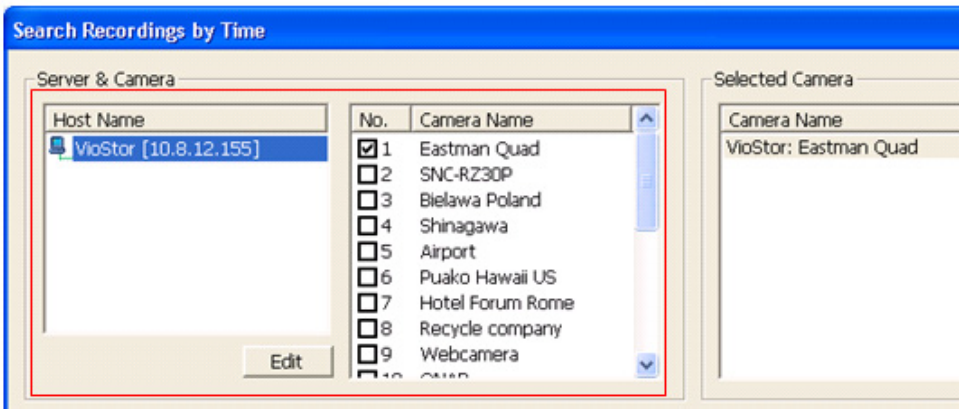
* You can select 4 IP cameras at maximum.



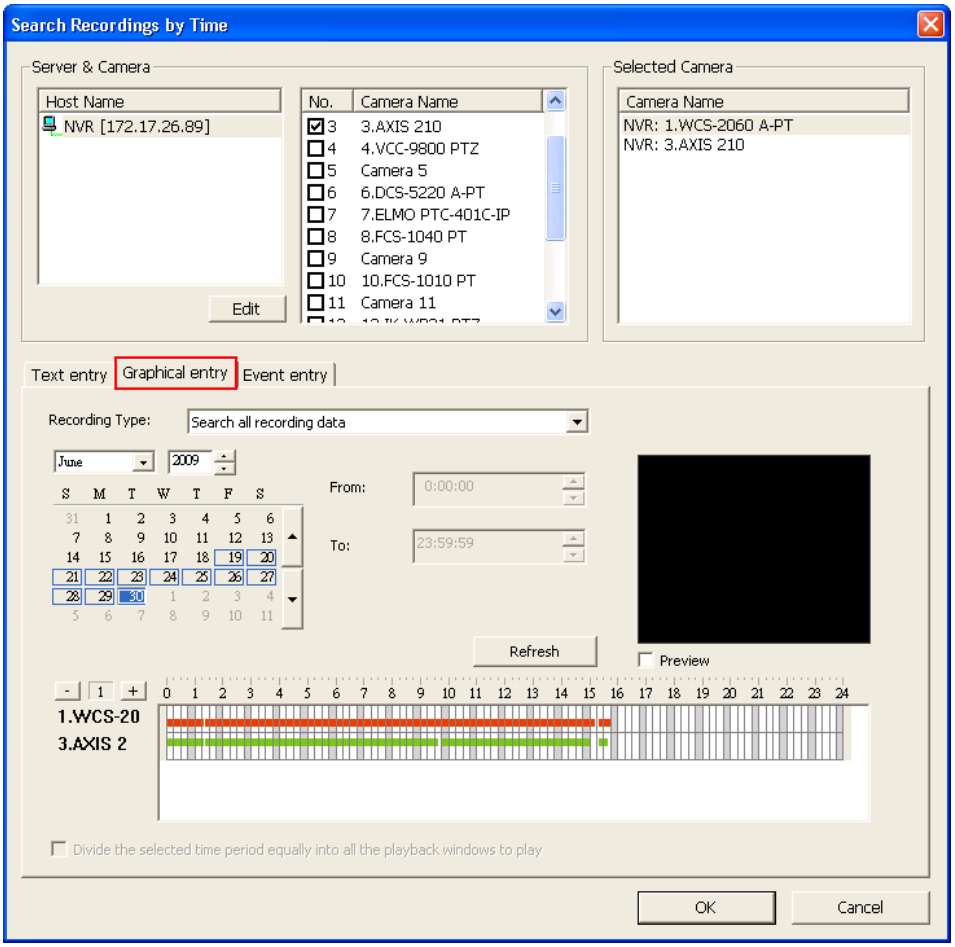
- **Timeline search**

  i. Select the server(s) and the IP camera(s)*.

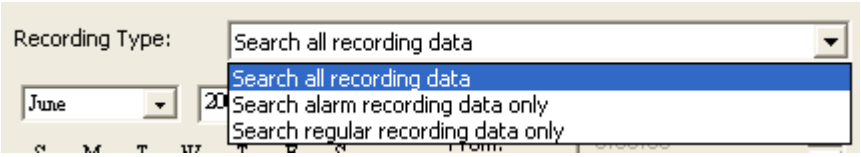
  * You can select 4 IP cameras at maximum.



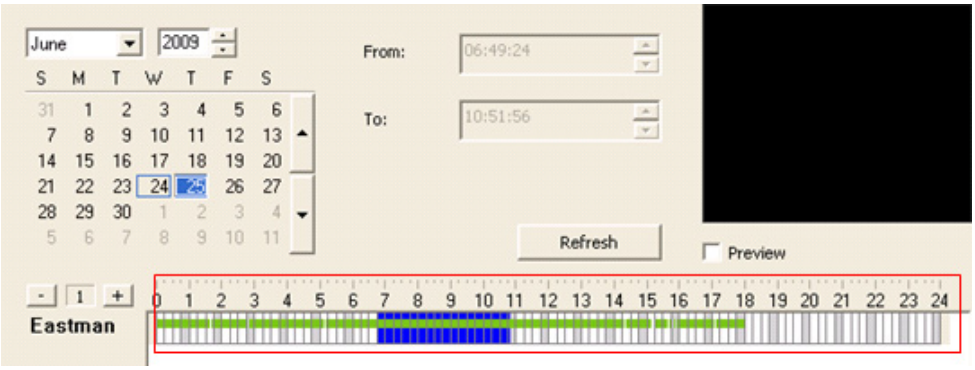
  ii. Click the "Graphical entry" tab.



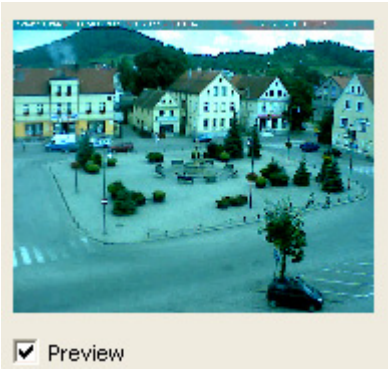
iii. Select the recording type.



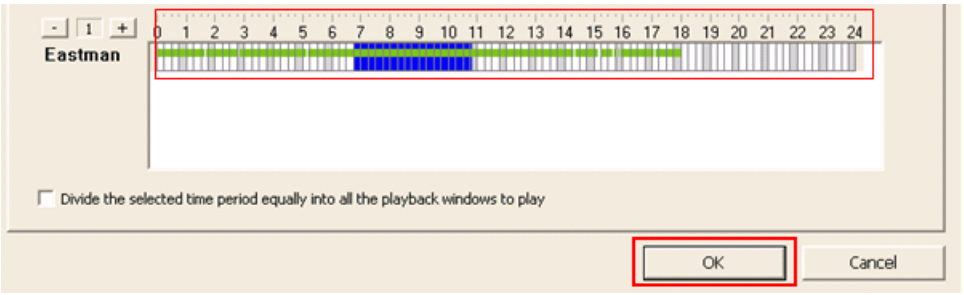
iv. Specify the time range when the files are recorded. The settings will be applied to all the cameras selected.



v. Click "Preview" to preview the searched video.



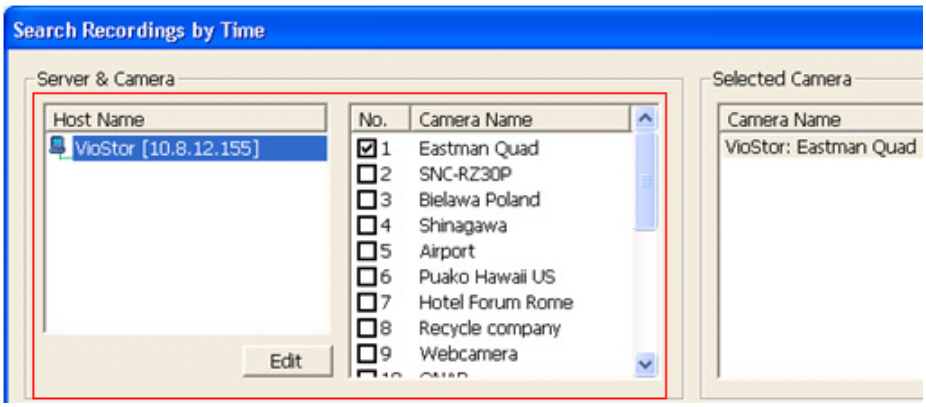
vi. Click "OK".



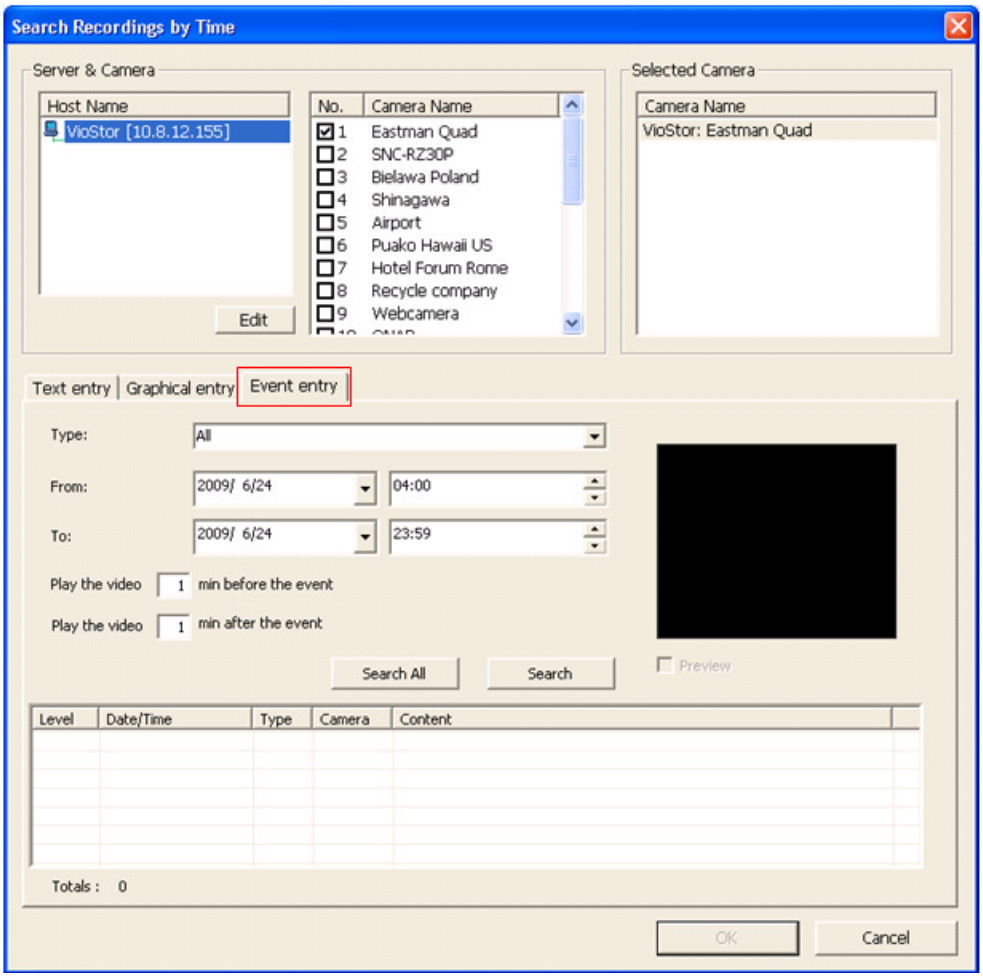
- **Event entry**

  i. Select the server(s) and the IP camera(s)*.

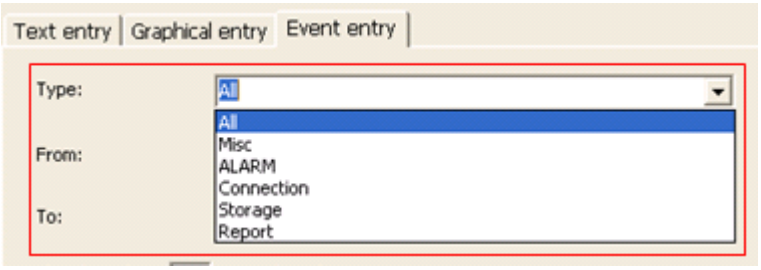
  * You can select 4 IP cameras at maximum.



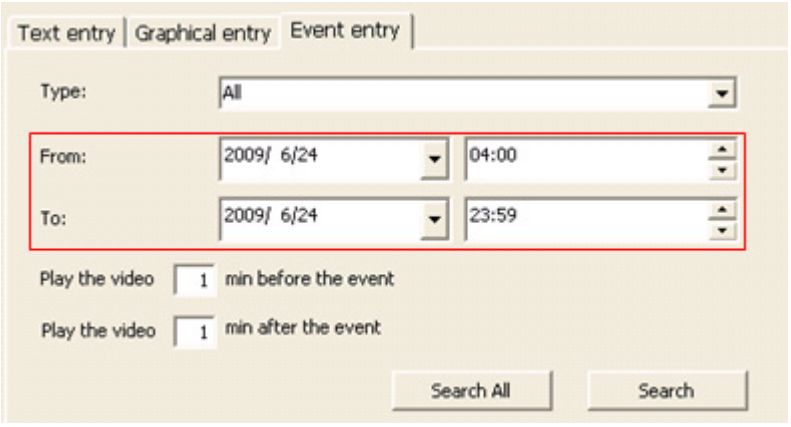
  ii. Click the "Event entry" tab.



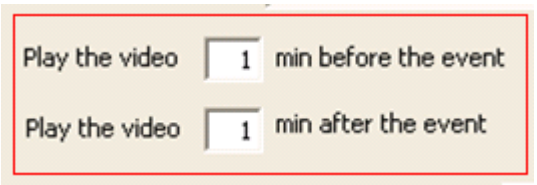
iii. Select the event type.



iv. Specify the time range when the files are recorded.

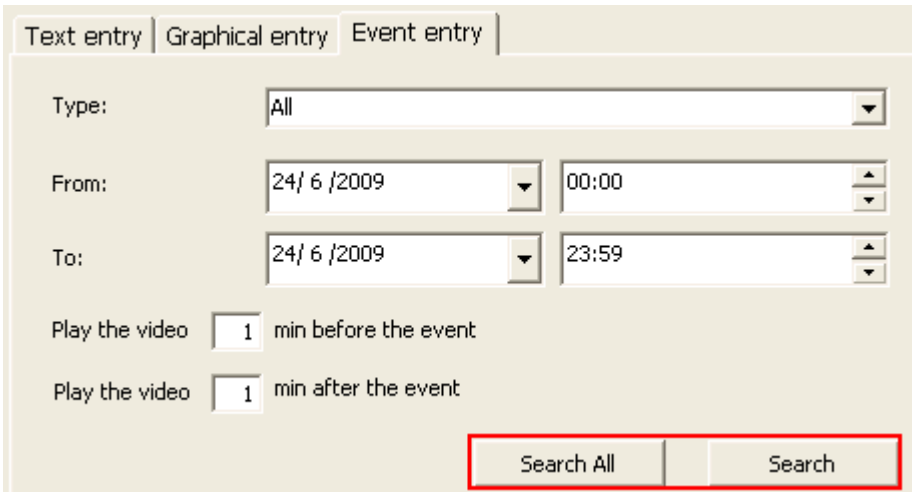


v. Specify the number of minutes for playing the video recorded before and after the event.



vi. Event search. This function is provided for you to search all the events occurred on the IP cameras. You may refer to the event details to search for the recording data.

- ✓ Search all: Search for the specified events occurred on all the IP cameras of an NVR within the time range specified.
- ✓ Search: Search for the specified events occurred on one IP camera within the time range specified.



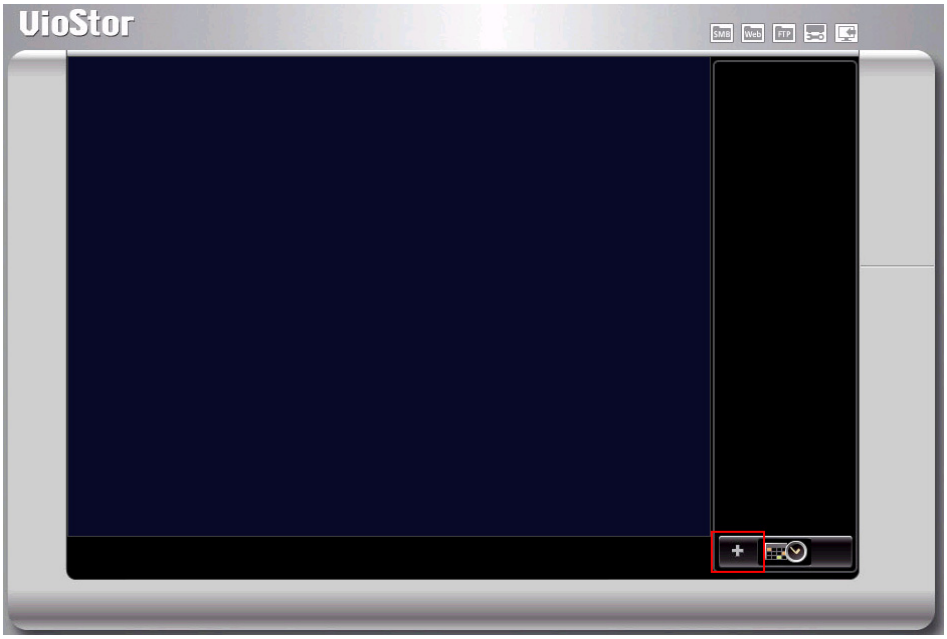
vii. The events will be shown. Click "OK".

5. When the files are shown, you can play the video. For further details of using the VioStor Player, click  to view the online help.

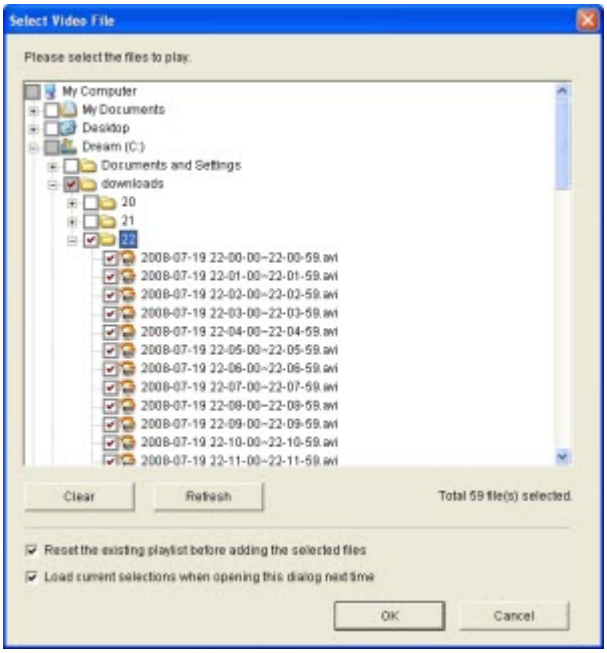
Note: The regular recordings are shown in white while the alarm recordings are shown in red on the playlist.

4.1.2 Play Video Files from Your Computer

1. Click "Add files"  .



2. Browse and select the files.



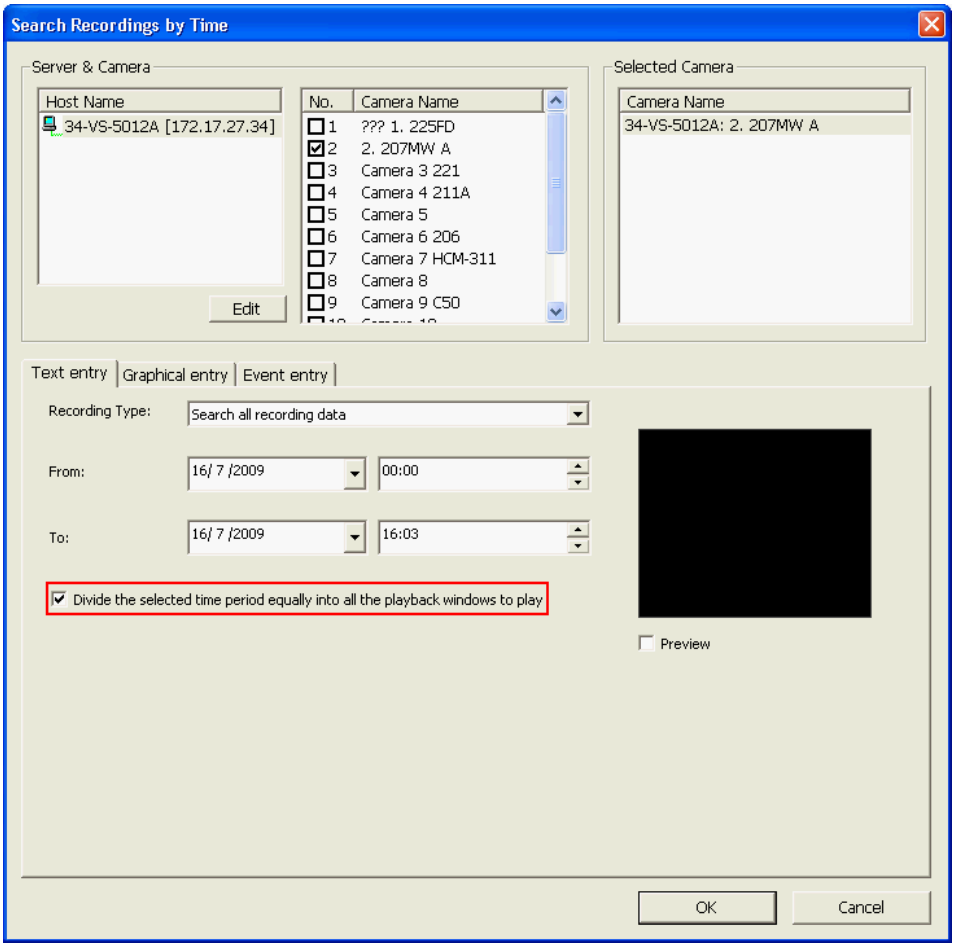
3. The playlist will be shown. Click "Play"  to start playing.

4.1.3 Quad-view Playback

Quad-view playback allows you to search for the video recorded by the NVR servers quickly. You can view the video of four IP cameras simultaneously or select to divide the video of one IP camera into four time periods and play them in a quad-view window.

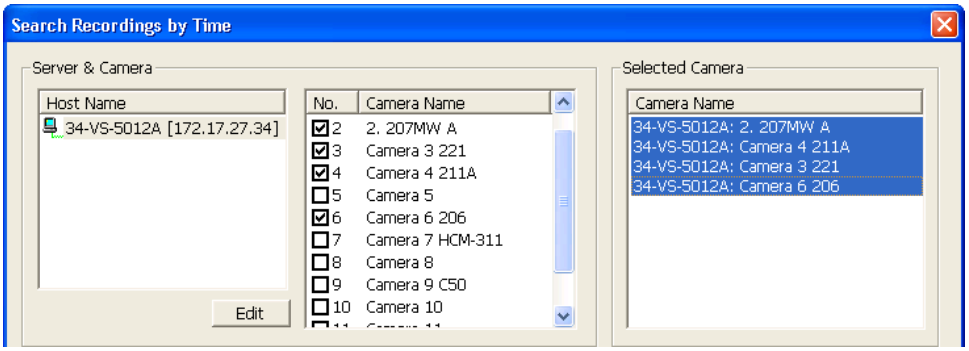
✓ **Divide the selected time equally into four playback windows**

Select only one camera. Click "Text entry" or "Graphical entry". Enter the search criteria and check the option "Divide the selected time period equally into all the playback windows to play". Click "OK".



✓ **Play the video of four IP cameras**

Select four IP cameras for video search. Enter the search criteria in "Text entry" or "Graphical entry". When the search results are shown, you can play the video files of the four IP cameras simultaneously.



4.1.4 Intelligent Video Analytics (IVA)

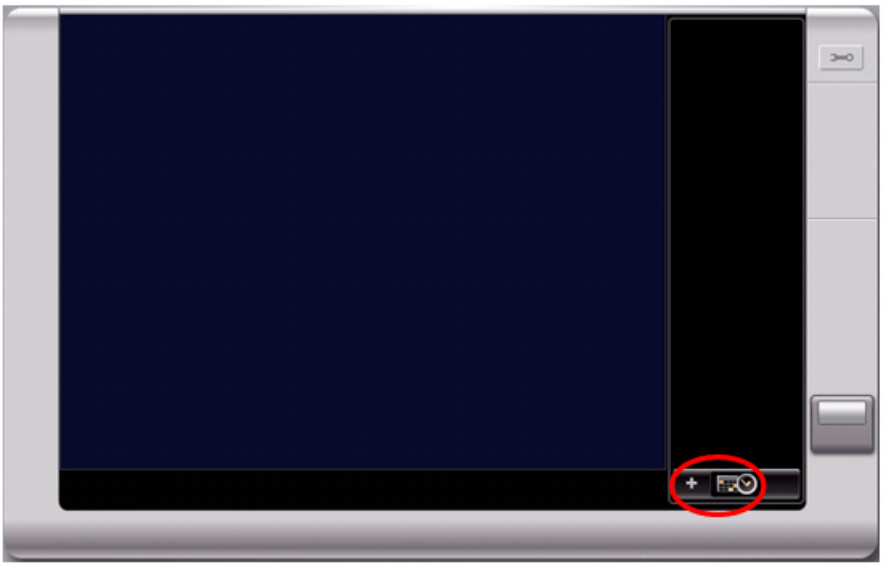
QNAP NVR supports intelligent video analytics to allow the users to search the video files efficiently. The time and effort for video search are largely reduced.

The following features are supported for video analytics:

- ✓ Motion detection: Detects movement of objects in the video.
- ✓ Foreign object: Detects new object in the video.
- ✓ Missing object: Detects missing object in the video.
- ✓ Out of focus: Detects out of focus of the camera in the video.
- ✓ Camera occlusion: Detects if the IP camera is obstructed.

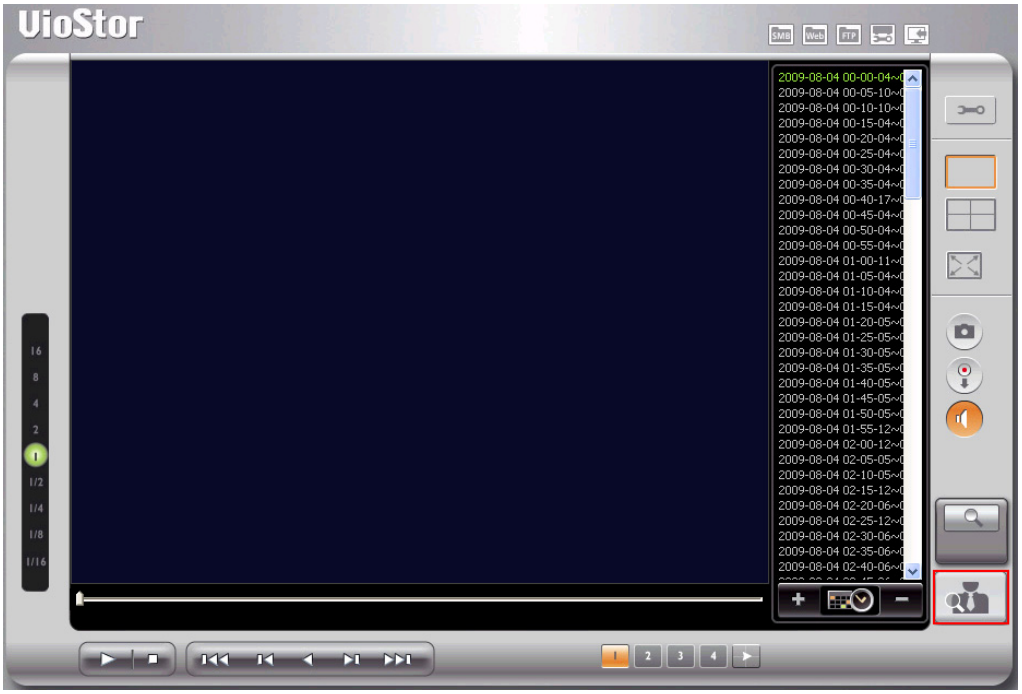
To use this function, follow the steps below:

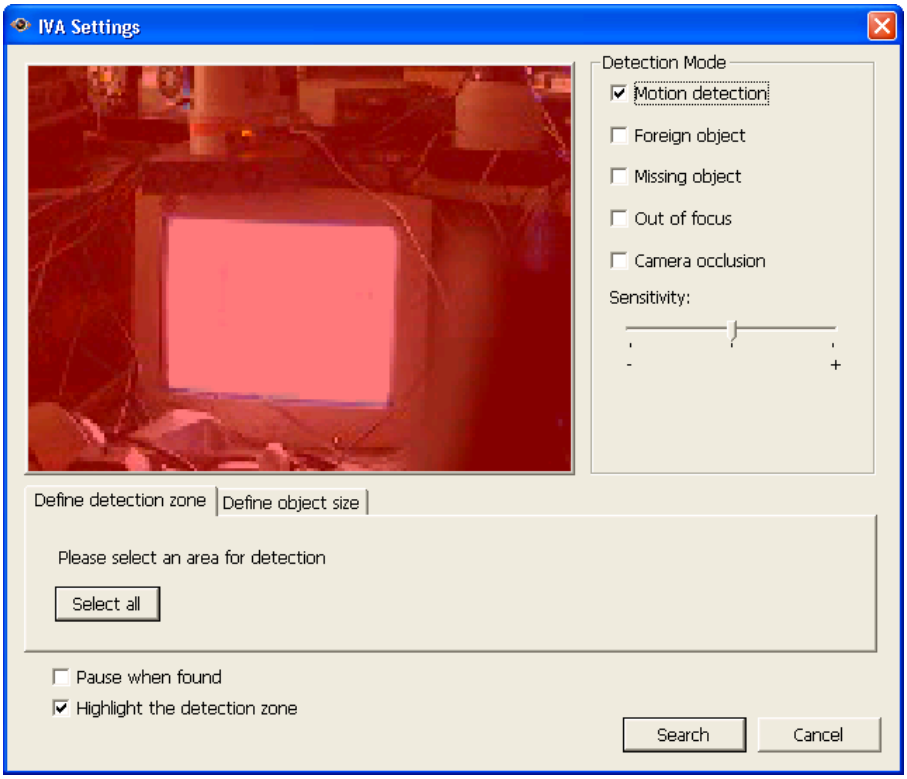
1. Go to Playback page of the NVR. Add files to the playlist.



Note: Intelligent video analytics support video search on one channel only.

2. On the playback window, click  .

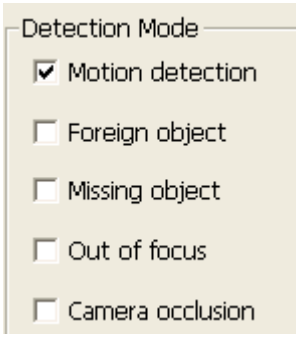




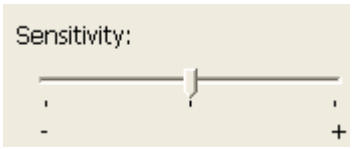
Note:

- ✓ When you check the option "Pause when found", the data search stops when a video file which matches the search criteria is found.
- ✓ When you enable "Highlight the detection zone", the moving objects will be highlighted in red brackets; the foreign or missing objects will be highlighted in yellow brackets; out of focus and camera occlusion will be displayed in transparent red.

3. Select the detection mode: motion detection, foreign object, missing object, out of focus, or camera occlusion. You can select multiple options.

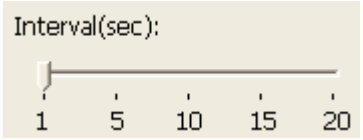


4. Adjust the sensitivity for object detection.

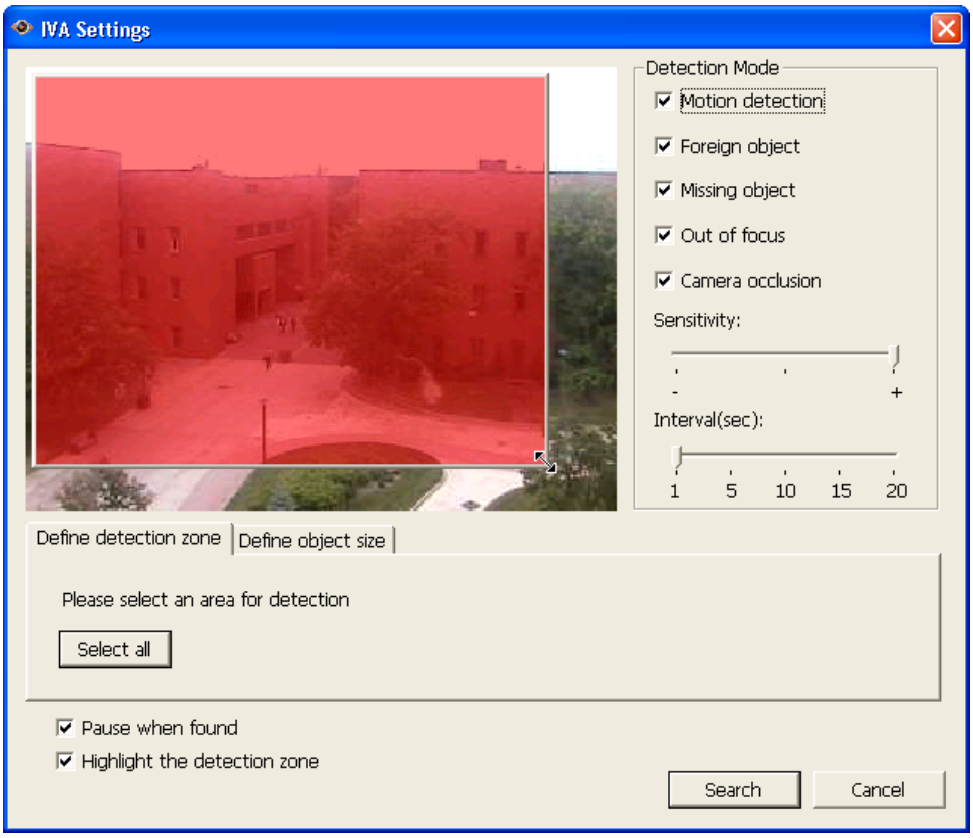


5. Adjust the time interval for foreign object and missing object. If a foreign object appears or a missing object disappears for a time period longer than the time interval, the system will record an event.

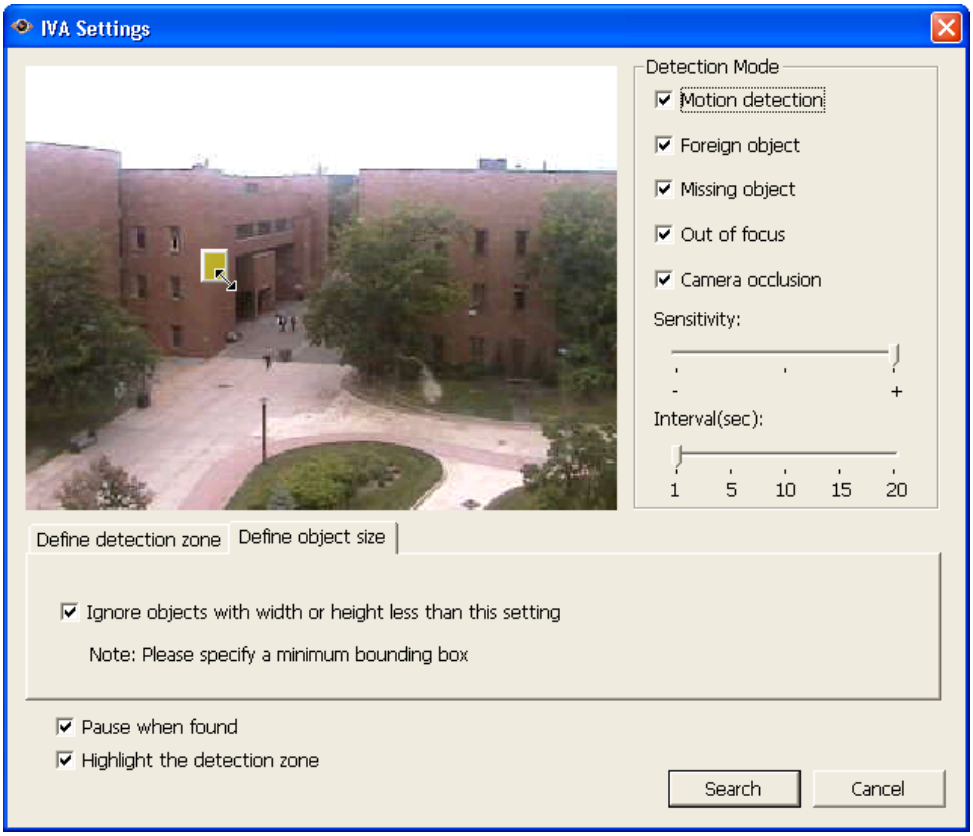
Note: The interval slide bar appears only when "foreign object" or "missing object" is checked.



6. Define detection zone. Mouse over the edge of the red zone and use the mouse to define the detection zone. Click "Select all" to highlight all the area for detection.

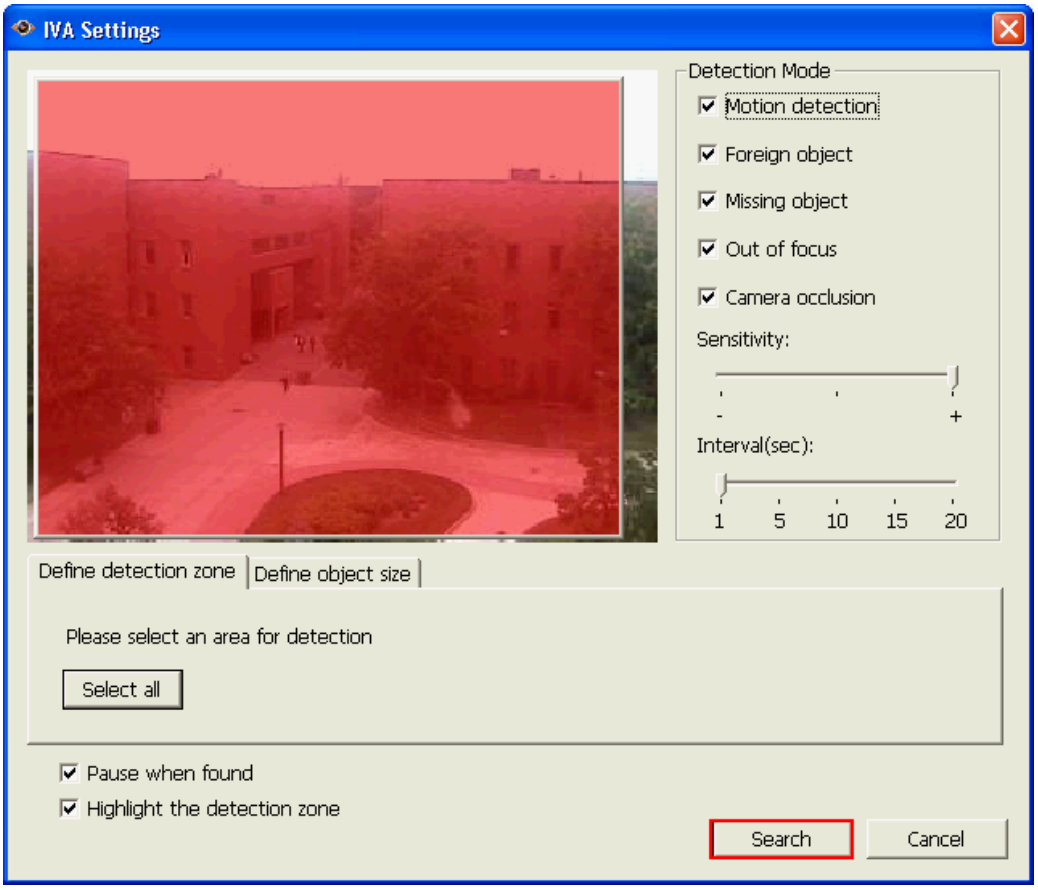


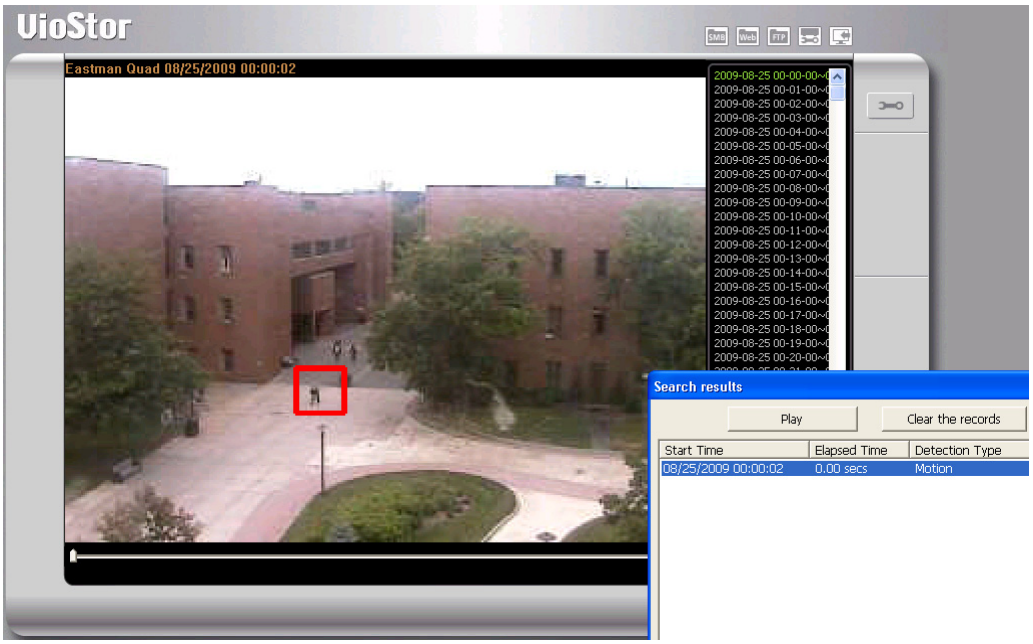
7. Define object size for the detection. You can use the mouse the drag the yellow zone to highlight the minimum object size for detection.



Note: After enabling this option, all the objects smaller than the yellow zone will be ignored for detection.

8. Click “Search” to start searching the video by IVA. The results and will be shown.





Note:

- You can double click an entry on the search result dialog to play the video. The player will play the video starting from 15 seconds before the event to 15 seconds after the event.
- You can also right click an entry on the search result dialog to export the video and save it on your computer. The exported video starts from 15 seconds before the event to 15 seconds after the event.

4.2 Digital Watermark

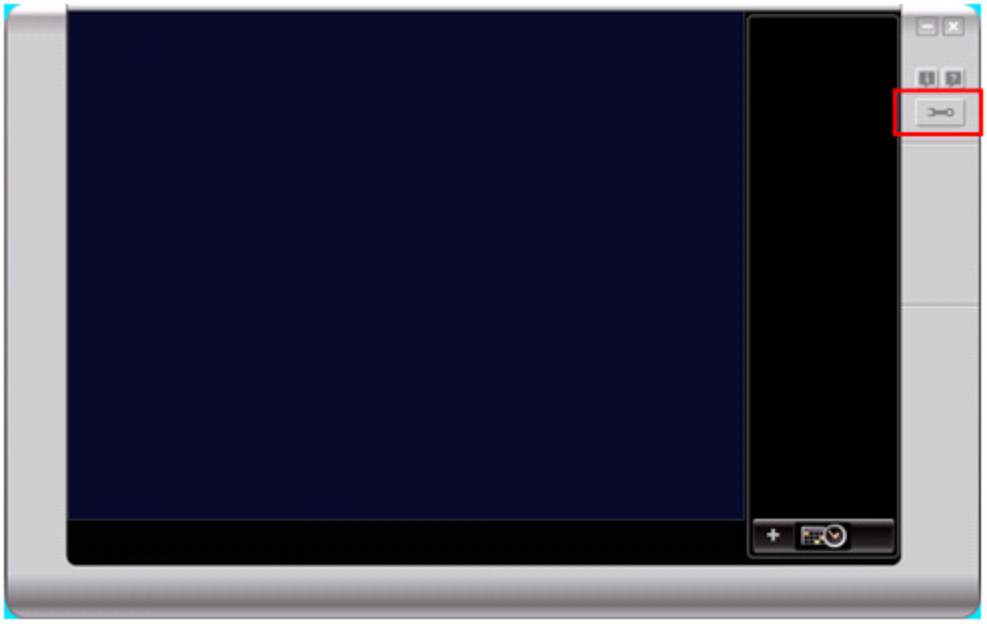
The VioStor NVR supports digital watermark to protect the videos and snapshots from unauthorized modification. You can select to add digital watermark on the exported video and snapshot on the VioStor Player. A permanent digital signal will be added to the exported files which are selected for digital watermarking. The watermark cannot be removed and is only visible by using watermark proof software.

4.2.1 Export Files with Digital Watermark

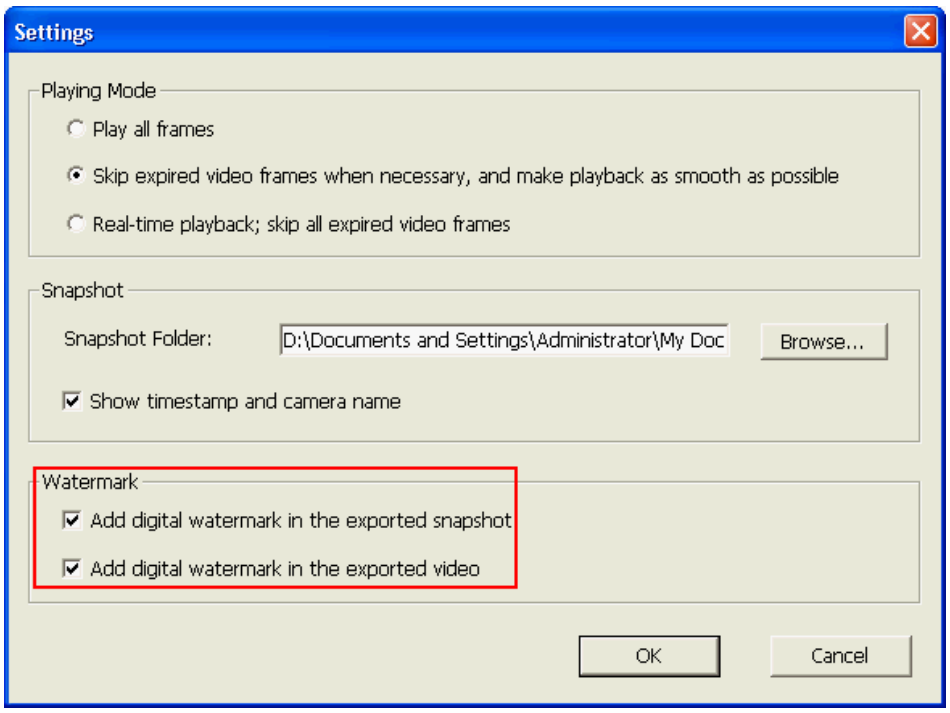
To use digital watermarking by VioStor Player, follow the steps below.

1. Click "Playback" to open the VioStor Player.

2. Click "Settings"  .



3. Select to add digital watermark in the exported snapshot or video.



4. Select the recording files (refer to Chapter 4).

5. Click  to convert the video files into avi format and enter the file name.

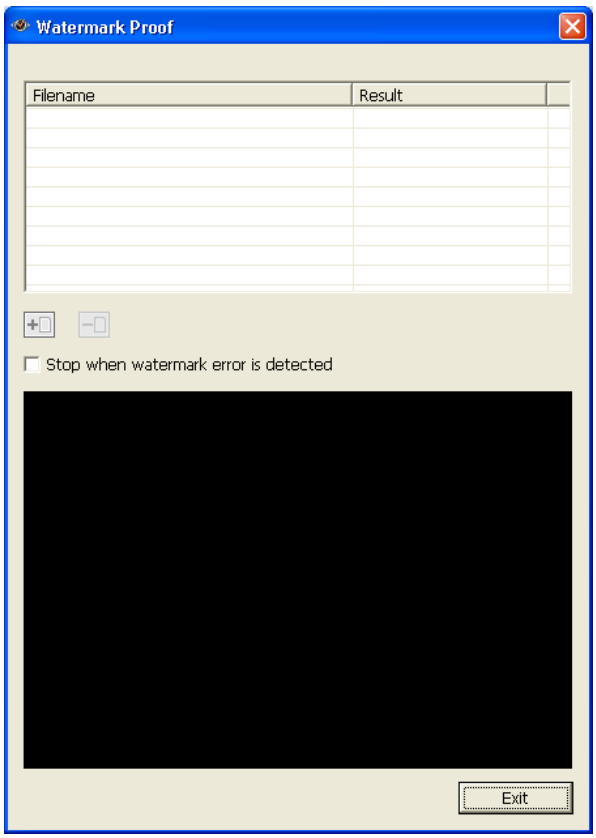
6. Click  to start playing and exporting the files.

Note: When you click  again, the NVR will stop exporting the files and resume to playback mode.

4.2.2 Watermark Proof

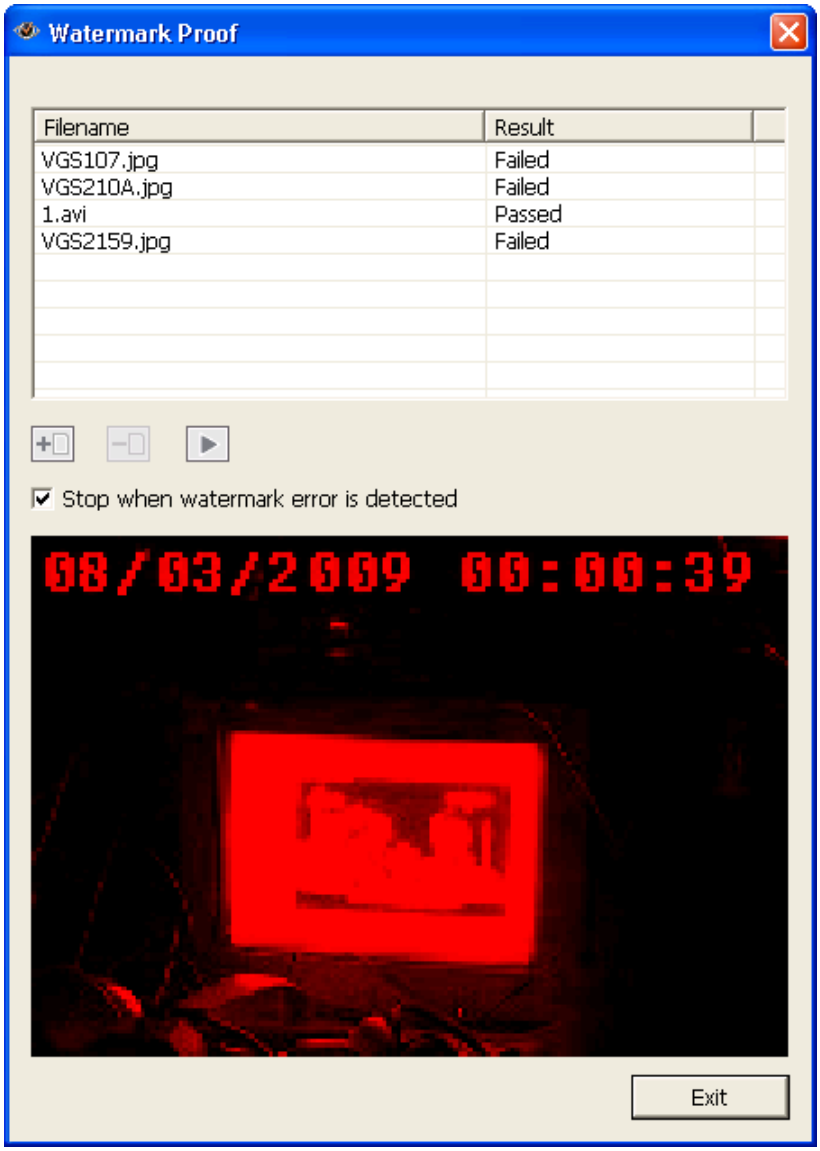
After installing the VioStor Player, Watermark Proof will be installed. From the Windows Start menu, select "All Programs" > "QNAP" > "Player" to locate "Watermark Proof".

Run Watermark Proof. The following window will be shown.



Click  to browse and locate the files. You can select more than one file at one time.

Click  to start checking the files. The Watermark Proof will start checking the files and show the proof result. If you check the option "Stop when watermark error is detected", the checking procedure will stop if a failed file is detected. Otherwise the program will check all the files you have selected. If a file is modified, the proof result will be shown as "Failed".



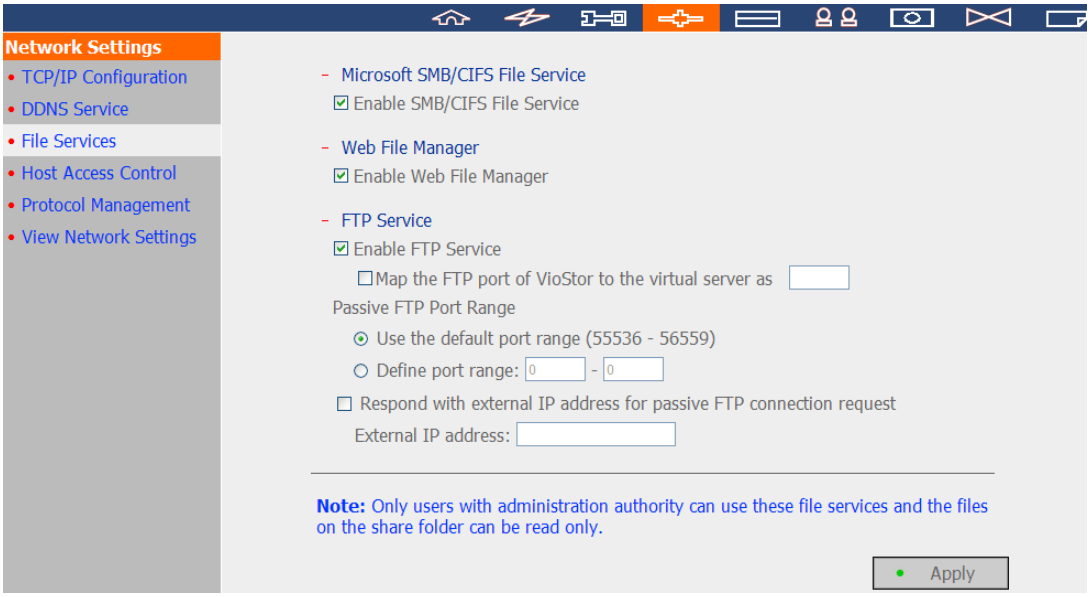
4.3 Access the Recording Data

You can access the recording data on the VioStor by the following network services:

- Windows Network Neighborhood (SMB/CIFS)
- Web File Manager (HTTP)
- FTP Server (FTP)

Note:

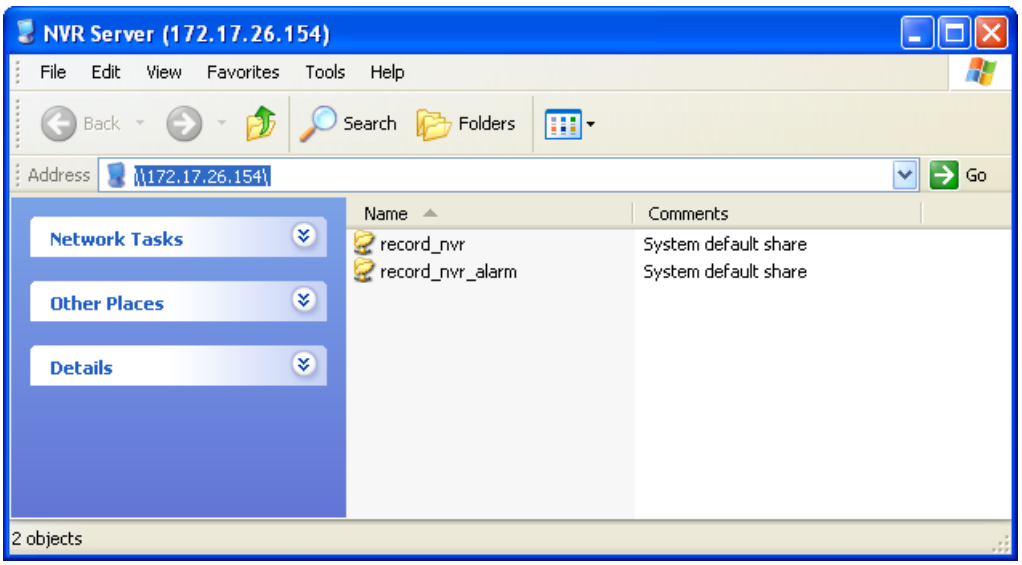
- To access the video file by these protocols, you must enter the user name and password with the administrator access right.
- To be able to use these services, enable the files services in "Network Settings" > "File Services" in the system administration page.



4.3.1 Windows Network Neighborhood (SMB/CIFS)

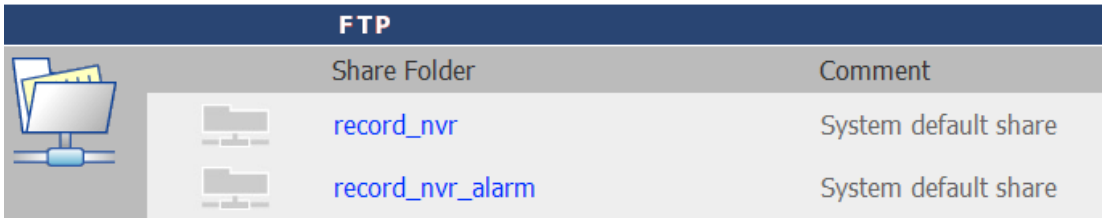
You can access recorded files by the SMB/CIFS protocol, which is popularly used in Windows system. You can connect to the recording folder by either:

- On the web-based playback interface, click "SMB".
- In Windows XP, run \\VioStorIP\ from the Start menu. For example, if your VioStor IP is 172.17.26.154, enter \\172.17.26.154.



4.3.2 Web File Manager (HTTP)

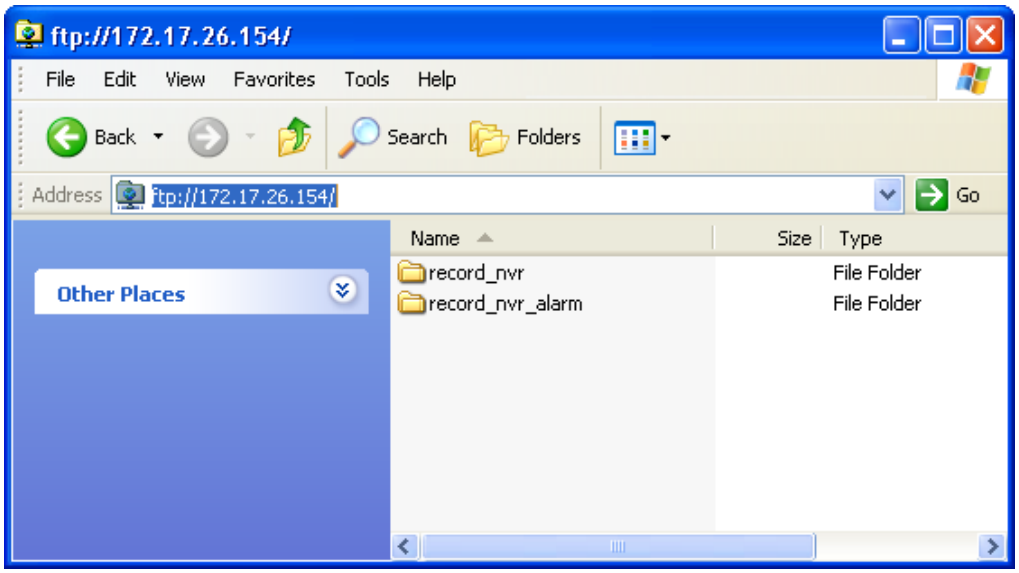
You can access the recording data from the web browser. On the web-based playback interface, click "Web".



4.3.3 FTP Server (FTP)

You can access the recording data by FTP:

- On the web-based playback interface, click "FTP".
- In Windows Internet Explorer, enter ftp://username:password@VioStorIP/. For example, enter ftp://admin:admin@172.17.26.154/ if the IP address of your VioStor is 172.17.26.154.



Chapter 5. System Administration

To login VioStor system configuration page, please login the monitoring page as an administrator and click .

The System Administration home page will be shown as below. An intuitive user interface is provided for the users to view the monitoring screens, connection and recording status, and network bandwidth.

	Preview	Camera Name	IP Address	Status	Recording status	Frame rate	Bit rate	Management
1		1. Panasonic HCM-481	172.17.27.134	Connected	Recording	10 fps	944.4 Kbps	
2		2. Axis Q7401	172.17.26.65	Connected	Recording	16 fps	435.9 Kbps	
3		3. Axis P3301	172.17.26.102	Connected	Recording	1 fps	122.7 Kbps	
4		4. i-Pro NS202	172.17.26.28	Connected	Recording	1 fps	232.9 Kbps	
5		5. IQeye 040S	172.17.27.24	Connected	Recording	13 fps	3606.8 Kbps	
6		6. IQeye 041S	172.17.27.25	Connected	Recording	2 fps	1795.5 Kbps	

If the system is not configured yet, the Quick Configuration page will be open to guide you through the setup steps first.

If there are questions, click on the help button  on the top right hand corner. The functions of the buttons are described below:

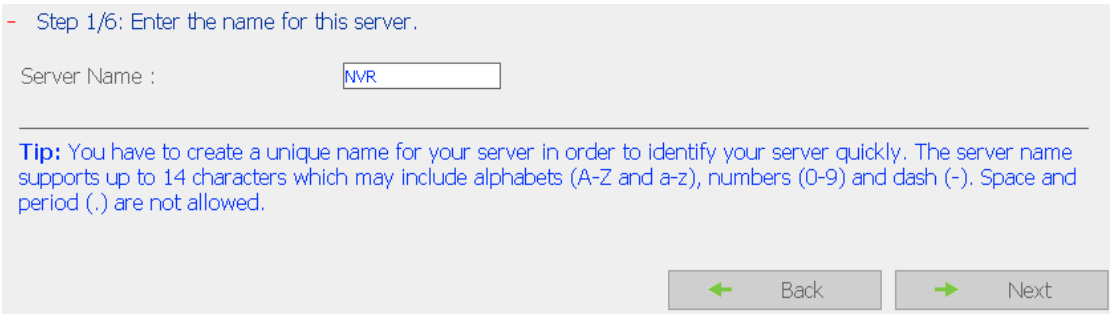
	Return to monitoring page
	Playback recorded video
	View On-line help
	Log out

5.1 Quick Configuration

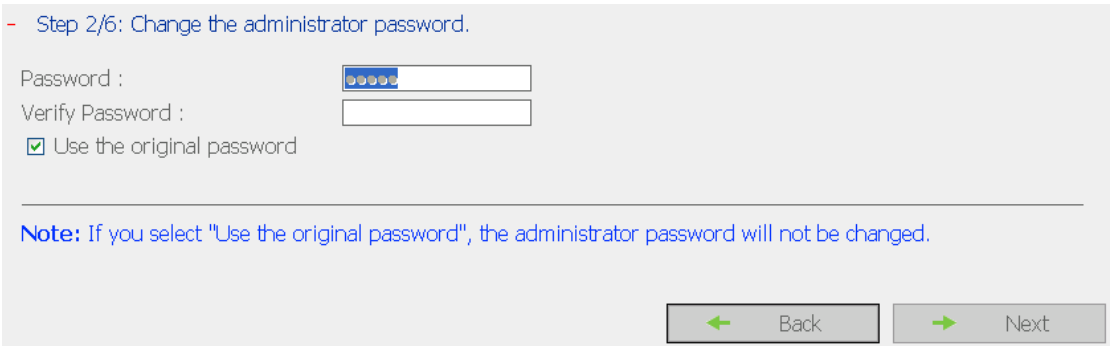
Please follow the instructions on the web page to configure VioStor.

Note: All changes to the settings will be effective only when the last step is applied.

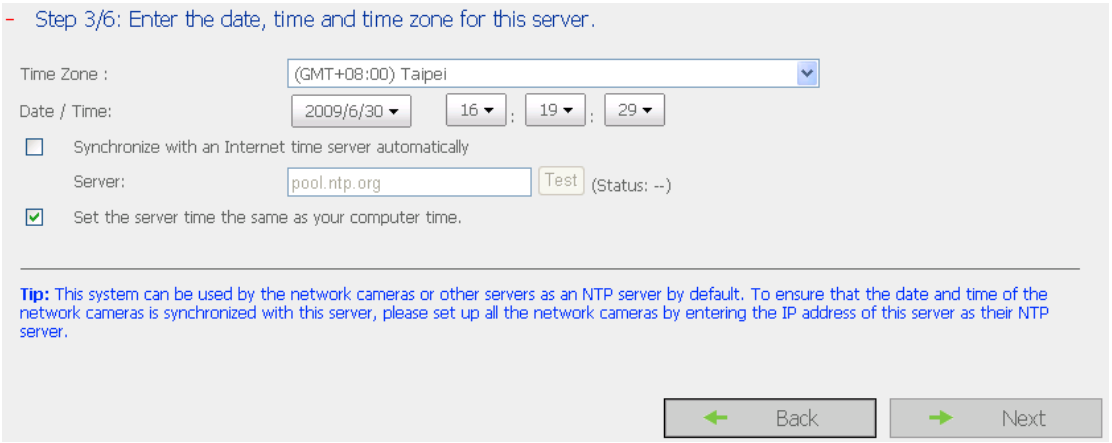
Step 1. Enter the server name.



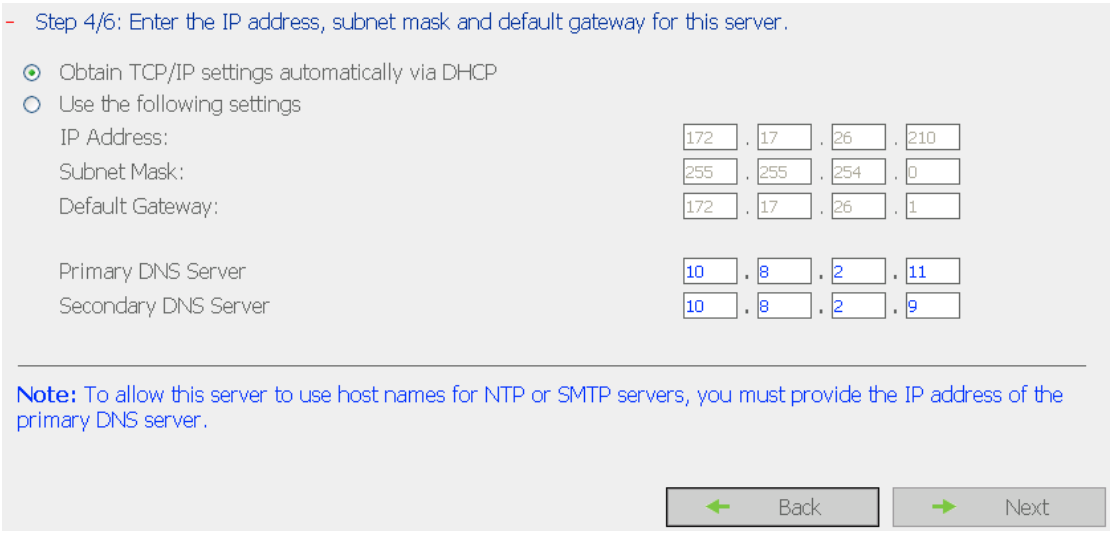
Step 2. Change the administrator password or select to use the original password.



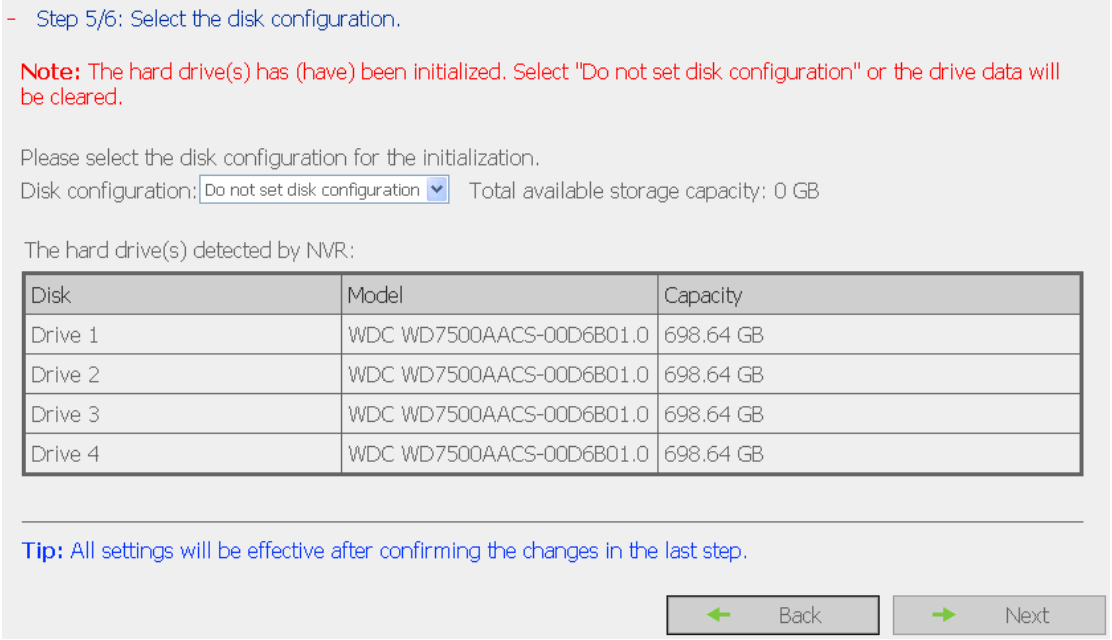
Step 3. Enter the date, time, and time zone of the server.



Step 4. Enter the IP address, subnet mask and default gateway of the server.



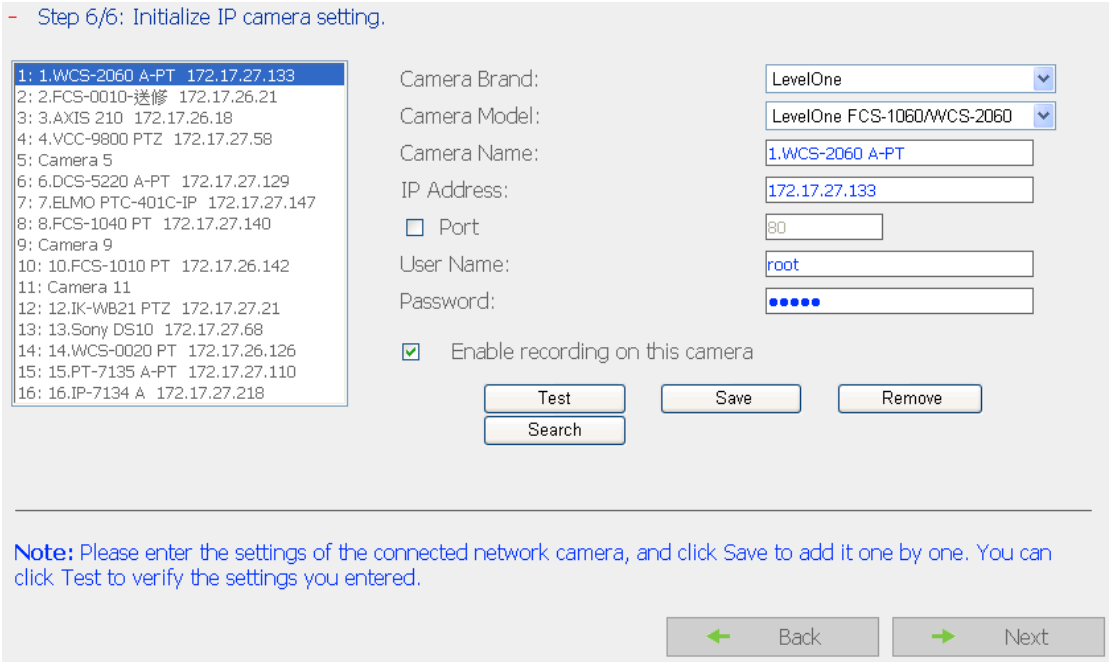
Step 5. Select the disk configuration to initialize the disk volume for the first time configuration. All data on the disk(s) will be deleted.



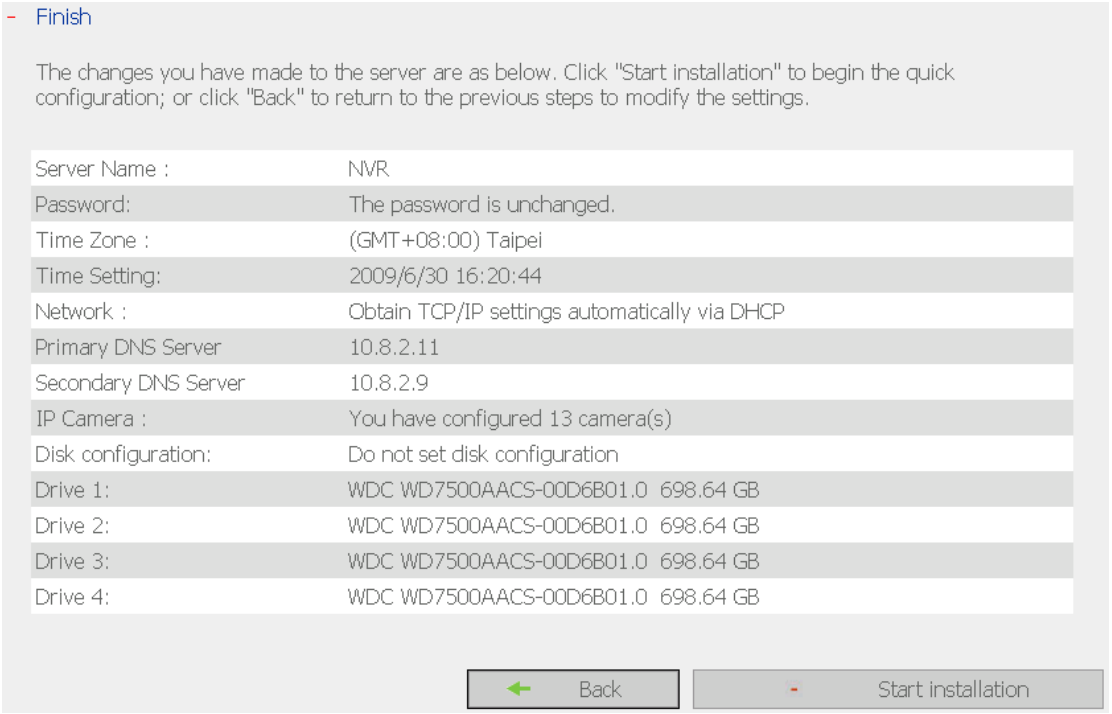
Step 6. Initialize IP camera setting.

Select the camera model; enter the camera name and IP address of the camera, and the user name and password to login the camera. You can also enable or disable recording on each camera, test connection to the cameras and then click "Save" to apply the changes.

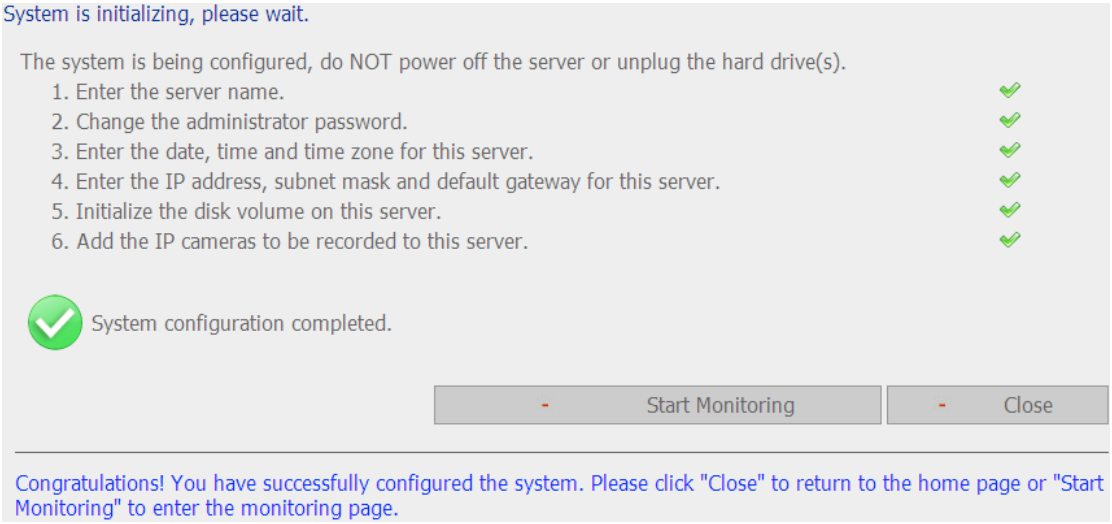
Click "Search" to search for the IP cameras in the local network. Select a channel for the camera and click "Add" to add the camera. By using the search function, the camera model and the IP address are filled in automatically. Click "Close" to close the search results.



After completing the settings, click “Start Installation” to apply the changes and initialize the system.



The quick configuration is completed and you can start to use the VioStor. Click “Start Monitoring” to view the live video from the cameras or click “Close” to return to the system administration home page.



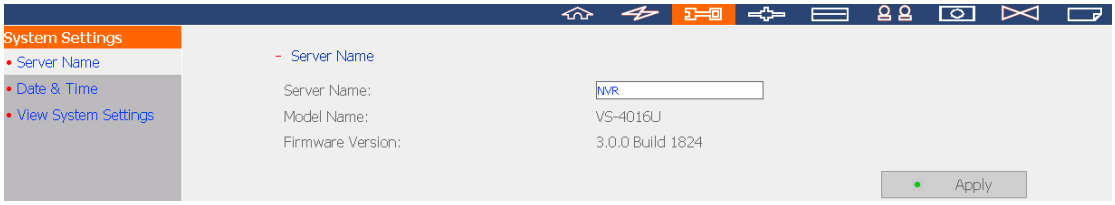
5.2 System Settings

You can configure the basic system settings including server name, date & time, and view the system settings.

5.2.1 Server Name

Enter the name of the VioStor. The server name is 14 characters long at maximum, which supports alphabets, numbers, and hyphen (-). The server does not accept names with space or names in pure number. The following characters are not supported.

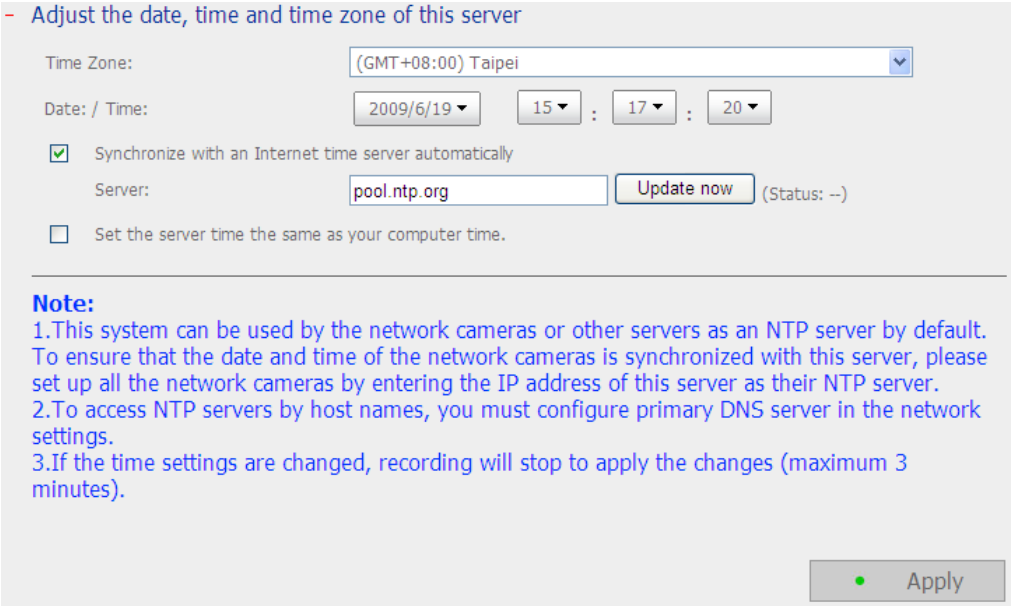
. ; : " < > * + = \ | ? , [ ] /



5.2.2 Date & Time

Set the date, time, and time zone according to your location. If the settings are incorrect, the following problems may occur:

- When playing the recorded video files, the display time will be incorrect.
- The time of event log displayed will be inconsistent with the actual time when an action occurs.



Synchronize with an Internet time server automatically

You can enable this option to update the date and time of the system automatically with specified NTP (Network Time Protocol) server. Enter the IP address or domain name of the NTP server, e.g. time.nist.gov, time.windows.com. Then enter the time interval for adjusting the time.

The VioStor can be used by the network cameras or other servers as an NTP server. To ensure the date and time of the network cameras are synchronized with this server, please set up all the network cameras by entering the IP address of the VioStor as their NTP server.

Note: The first time you enable NTP server, it may take several minutes for time synchronization before the time is correctly adjusted.

5.2.3 View System Settings

You can view the system settings, e.g. server name, on this page.

5.3 Network Settings

You can configure the WAN and LAN settings, DDNS service, file service, host access control, protocol management and view the network settings in this section.

5.3.1 TCP/IP Configuration

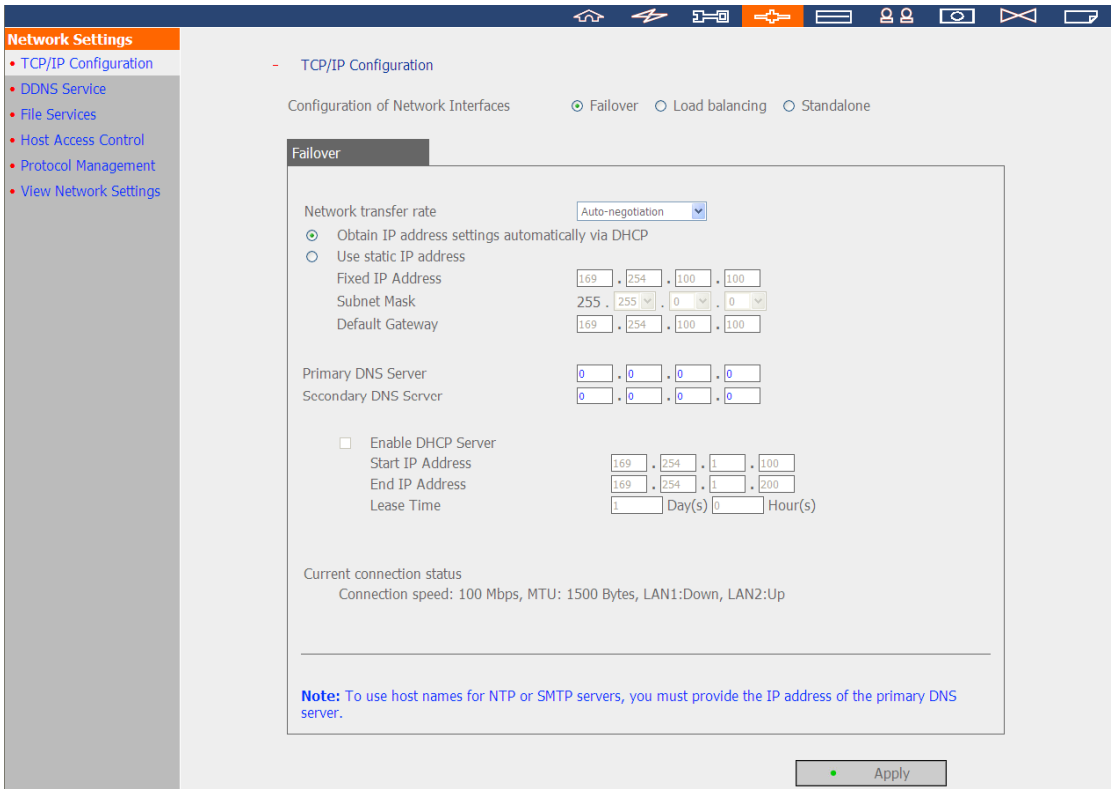
You can select one of the following two methods to configure the TCP/IP settings of the NVR.

- **Obtain IP address settings automatically via DHCP**
  If your network supports DHCP, the NVR will use DHCP protocol to retrieve the IP address and related information automatically.
- **Use static IP address**
  To use fixed IP address for network connection, enter fixed IP address, subnet mask, and default gateway.

Primary DNS Server: Enter the IP address of primary DNS server that provides DNS service for the NVR in external network.
Secondary DNS Server: Enter the IP address of secondary DNS server that provides DNS service for the NVR in external network.

Note: Jumbo Frame setting is valid in Gigabit network environment only. Besides, all network appliances connected must enable Jumbo Frame and use the same MTU value.

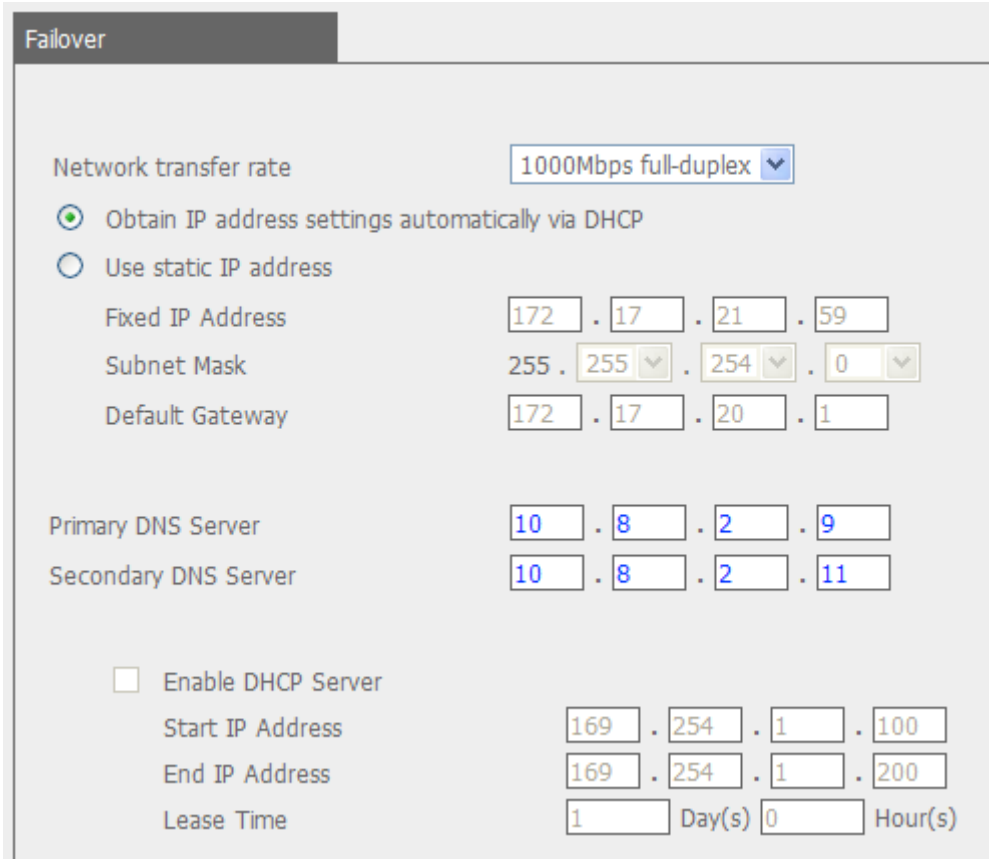
If your system supports 2 LAN ports, you can select to use failover, load balancing, or standalone settings. To use these features, make sure both LAN ports are connected to the network.



Configuration of Network Interfaces

- **Failover (Default settings for dual LAN NVR models)**

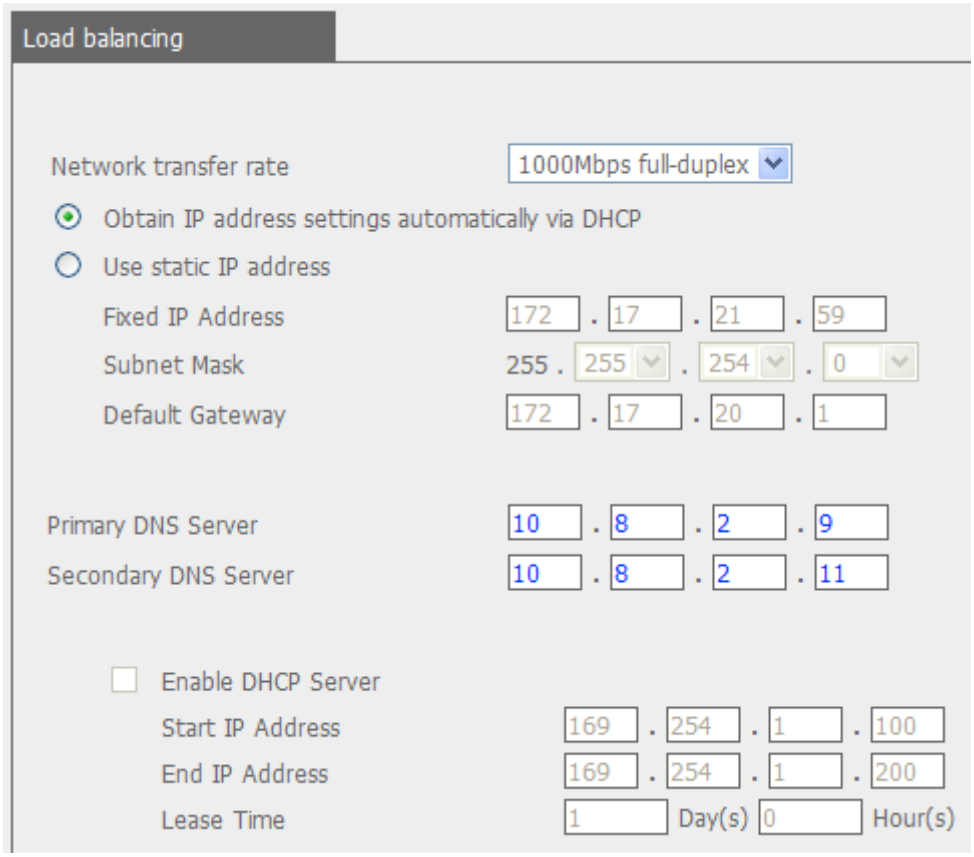
  Failover refers to the capability of switching over the network transfer port to the redundant port automatically when the primary one fails due to hardware or connection error to avoid network disconnection. When the primary network port resumes to work, the network transfer will be switched back to that port automatically.



- **Load balancing**

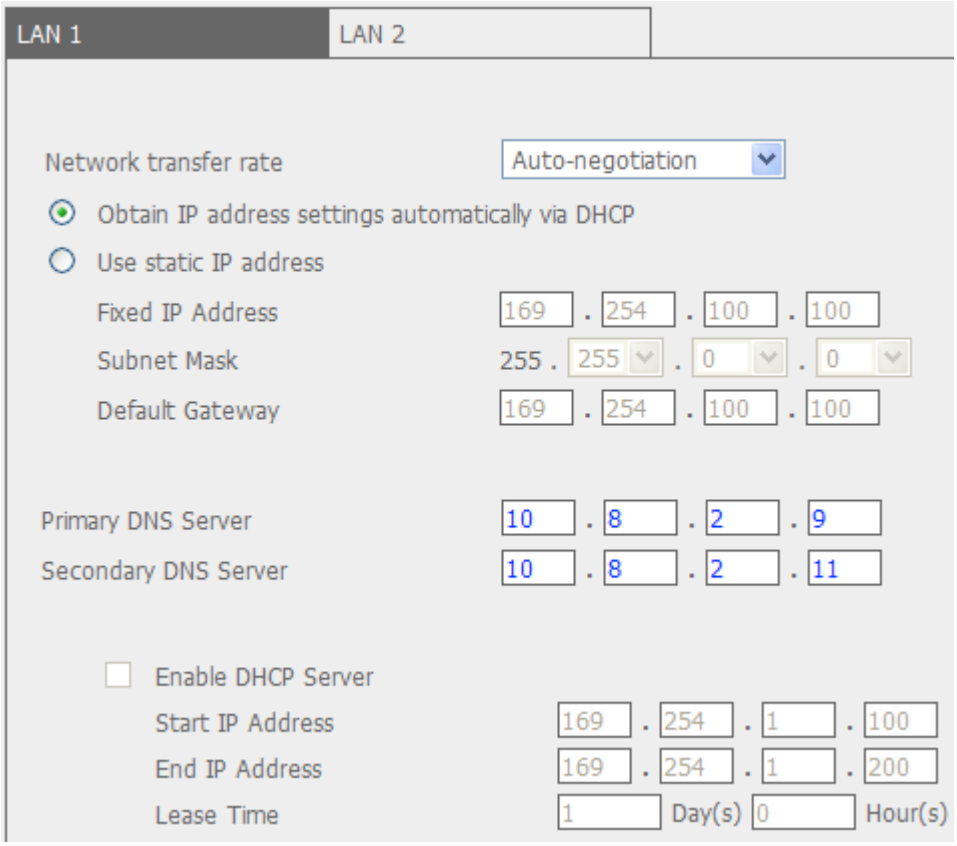
  Load balancing enables the network resources to spread between two or more network interfaces to optimize network transfer and enhance system performance. It operates on layer 3 protocol (IP, NCP IPX) only. Multicast/ broadcast and other non-routable protocols, e.g. NetBEUI, can only be transferred via the main network port.

Note: To optimize the network transfer speed of the VioStor in load balancing mode, please use a managed Ethernet switch and enable 802.3ad (or link aggregation) on the ports of the switch that the Giga LAN ports of the VioStor are connected to.



- **Standalone**

  The standalone option allows you to assign different IP settings for each network port. The VioStor can be accessed by different workgroups in two different subnets. However, when this function is enabled, failover does not work. You can only enable DHCP server for the primary network port (LAN 1).



- **Network Transfer Rate**

  You can select auto-negotiation (default), 1000 Mbps, or 100 Mbps. It is recommended to use the default setting that the server will determine network speed automatically.
- **Obtain IP address settings automatically via DHCP**

  If your network supports DHCP, VioStor will use DHCP protocol to retrieve the IP address and related information automatically.
- **Use static IP address**

  To use fixed IP address for network connection, enter fixed IP address, subnet mask, and default gateway.
- **Primary DNS Server**

  Enter the IP address of primary DNS server that provides DNS service for VioStor in external network.

- **Secondary DNS Server**
  Enter the IP address of secondary DNS server that provides DNS service for VioStor in external network.

Enable DHCP Server

If no DHCP is available in the LAN where the VioStor locates, you can enable this function to enable the VioStor as a DHCP server and allocate dynamic IP address to DHCP clients in LAN.

You can set the range of IP addresses allocated by DHCP server and the lease time. Lease time refers to time that IP address is leased to the clients by DHCP server. When the time expires, the client has to acquire an IP address again.

Note: If there is an existing DHCP server in your LAN, do not enable this function. Otherwise, there will be IP address allocation and network access errors.

5.3.2 DDNS (Dynamic Domain Name) Service

The DDNS service enables users to connect VioStor via domain name directly. There is no need to memorize the lengthy IP address of the server. To enable the DDNS service, you have to register a DDNS account from a DDNS provider. Please refer to Appendix A.

The VioStor currently supports the DDNS service provided by:

1. DynDNS (http://www.dyndns.org/)
2. update.ods.org
3. members.dhs.org
4. www.dyns.cx
5. www.3322.org
6. www.no-ip.com
7. ipcam.jp

5.3.3 File Services

You can enable the SMB/ CIFS file service, Web File Manager and FTP service to access the recorded video files. These settings are enabled by default.

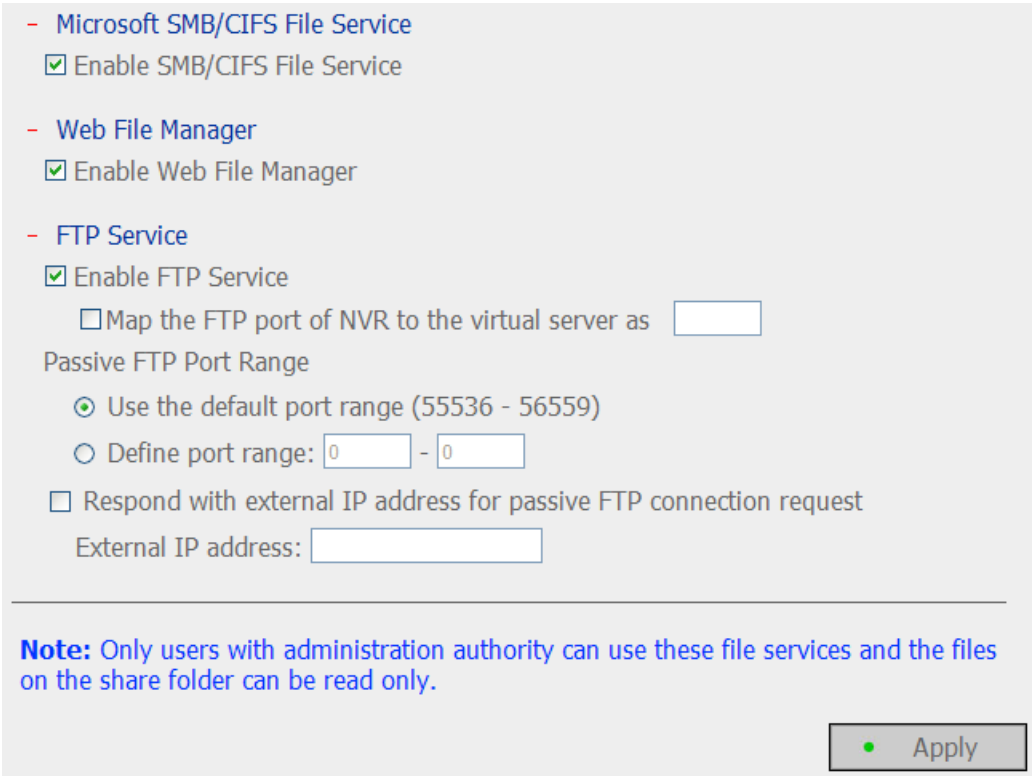
If your VioStor is installed behind the router, you could enable FTP port mapping, so that users from the external network can access the VioStor via FTP (please refer to Appendix B).

Passive FTP Port Range

You can use the default port range (55536-56559) or define a port range larger than 1023. When using this function, make sure you have opened the configured port range on your router or firewall.

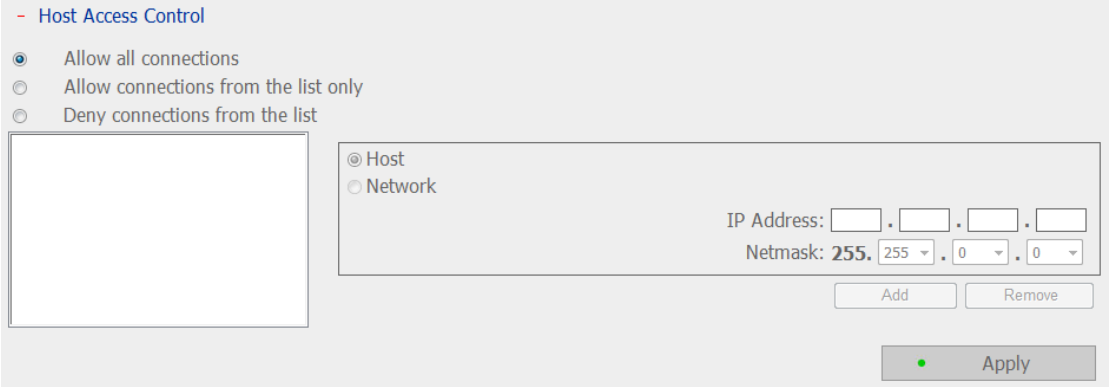
Respond with external IP address for passive FTP connection request

When passive FTP connection is in use and the VioStor is configured under a router, if the remote computer cannot connect to the VioStor via WAN, you can enable this function. By enabling this function, the FTP service replies the manually specified IP address or automatically detects the external IP address so that the remote computer can connect to the VioStor successfully.



5.3.4 Host Access Control

Specify the connections to be allowed and denied to access the VioStor. Choose one of the following options to restrict access from a network or an IP address (host) to the server:



1. Allow all connections (Default setting)

Allow connection from all hosts to the server.

2. Allow connections from the list only

Allow connection from hosts specified on the list only.

> **Note:** When this function is enabled, you can only use PC that the IP address is listed on the connection list to connect or find the VioStor. The IP address not included in the list will not be able to detect the VioStor not listed in allowed connections.

3. Deny connections from the list

Deny connection from hosts specified on the list.

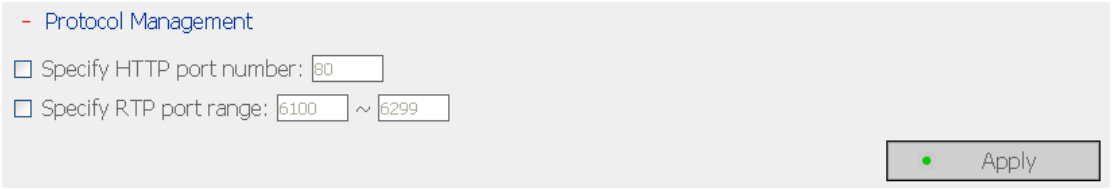
> **Note:** Make sure your PC is added in the list of hosts allowed to connect to the server. Otherwise, the VioStor will disconnect your PC when you apply the new settings.

5.3.5 Protocol Management

To assign a specific port for accessing the VioStor by the web browser, please enable the option "Specify HTTP port number" and enter the port number. The default setting is 80.

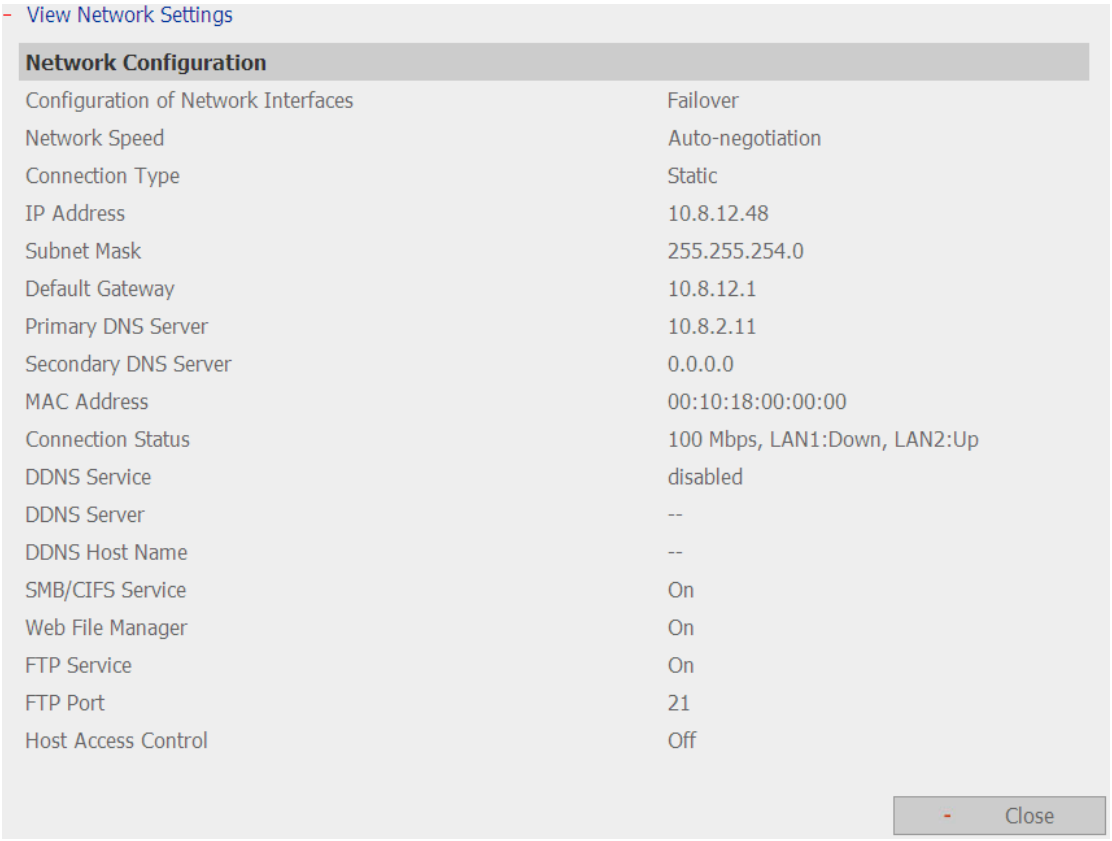
RTP (Real-time Transfer Protocol) is a standardized packet format for delivering real-time audio and video data of network cameras over the Internet. The real-time data transfer is monitored and controlled by RTP (also RTCP). The default setting is 6100-6299. If your network cameras use different RTP ports, please enable "Specify RTP port range" and enter the port numbers.

Note: Make sure you have opened the ports you set on the router or firewall to ensure normal monitoring and recording.



5.3.6 View Network Settings

You can view current network settings and status of VioStor in this section.



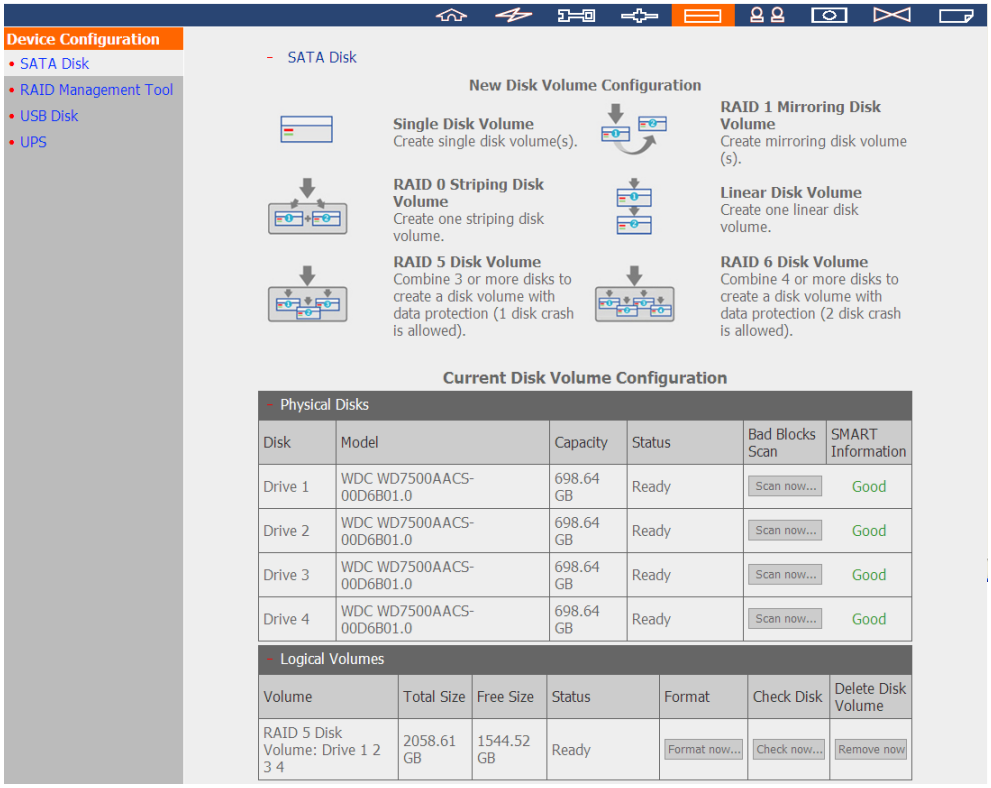
5.4 Device Configuration

You can configure SATA disk, RAID management tool, USB disk, and UPS settings in this section.

5.4.1 SATA Disk

This page shows the model, size and current status of the disk(s) installed on the VioStor. You can format and check disks, and scan bad blocks on the disks. When the SATA disks are formatted, the VioStor will create the following default share folders:

- record_nvr: The folder for saving regular recording files
- record_nvr_alarm: The folder for alarm recording



Disk Configuration	Applied NVR Models
Single disk volume	All models
RAID 1, JBOD (just a bunch of disks)	2-bay models or above
RAID 5, RAID 6, RAID 5+hot spare,	4-bay models or above
RAID 6+hot spare	5-bay models or above

You can create the disk volume of the following type:

- **Single Disk Volume**
  Each disk will be used as a standalone disk. However, if a disk is damaged, all data will be lost.

- **RAID 1 Mirroring Disk Volume**
  RAID 1 (mirroring disk) protects your data by automatically backing up the contents of one drive onto the second drive of a mirrored pair. This protects your data if one of the drives fails. Unfortunately, the storing capacity is equal to a single drive, as the second drive is used to automatically back up the first. Mirroring Disk is suitable for personal or corporate use to store important data.

- **RAID 0 Striping Disk Volume**
  RAID 0 (striping disk) combines 2 or more drives into one larger disk. It offers the fastest disk access but it does not have any protection of your data if the striped array fails. The disk capacity equals the number of drives in the array times the size of the smallest drive. Striping disk is usually used to maximize your disk capacity or for fast disk access but not for storing important data.

- **Linear Disk Volume**
  You can combine two or more disks into one larger disk. During file saving, the file will be saved on physical disks sequentially but does not have a disk failure file protection function. The overall capacity of linear disk is the sum of all disks. Linear disk is generally used for storing large data and is not appropriate to use for file protection of sensitive data.

- **RAID 5 Disk Volume**
  RAID 5 disk volume is ideal for organizations running databases and other transaction-based applications that require storage efficiency and data protection.
  To create a RAID 5 disk volume, a minimum of 3 hard disks are required. The total capacity of RAID 5 disk volume = the size of the smallest capacity disk in the array x (no. of hard disk – 1). It's recommended that you use the same brand and same capacity hard drive to establish the most efficient hard drive capacity.
  Additionally, if your system contains four disk drives, three of them can be used

to implement RAID 5 data disks and the fourth drive can be used as a spare disk. When a physical disk failure occurs, the system will automatically rebuild the data with the spare disk.

RAID 5 can survive 1 disk failure and system can still operate properly. When a disk fails in RAID 5, the disk volume will be in "degraded mode". There is no more data protection at this stage. If one more disk fails, all the data will be crashed. Therefore, you must replace a new disk immediately. You can install a new disk after turning off the server or hot swap the new disk when the server is on. The status of the disk volume will become "rebuilding" after installing a new disk. When rebuilding completes, your disk volume resumes to normal status.

Note: To install a disk when the server is on, make sure the disk volume is in "degraded" mode. Or wait for two long beeps after the disk crash, then insert the new disk.

- **RAID 6 Disk Volume**

  RAID 6 disk volume is ideal for important data protection.

  To create a RAID 6 disk volume, a minimum of 4 hard disks are required. The total capacity of RAID 6 disk volume = the size of the smallest capacity disk in the array x (no. of hard disk–2). It's recommended that you use same brand and same capacity hard drive to establish the most efficient hard drive capacity.

  RAID 6 can survive 2 drives failure and system can still operate properly.

  Note: To install a disk when the server is on, make sure the disk volume is in "degraded" mode. Or wait for two long beeps after the disk crash, and then insert the new disk.

- **RAID 5, RAID 6 Read-only Mode**

  The drive configuration enters read-only mode in the following occasions:

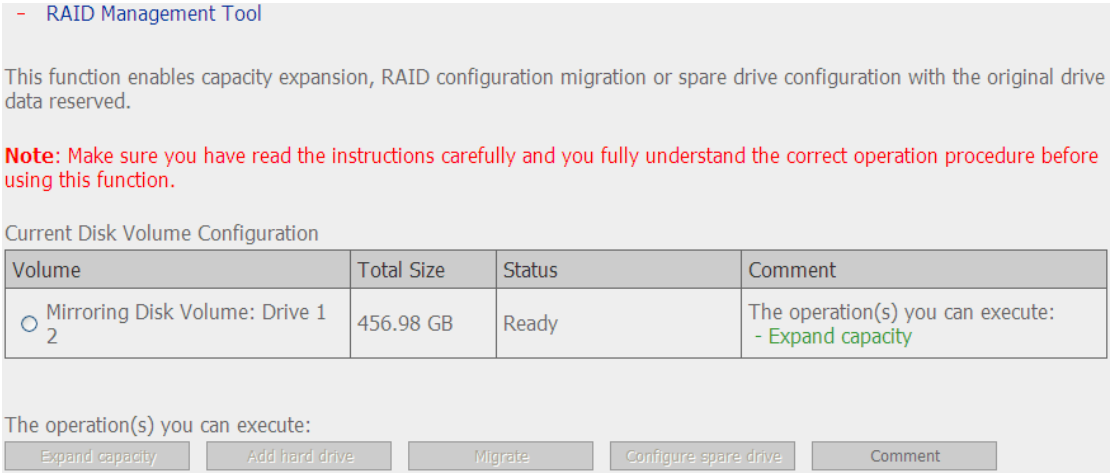
  - 2 drives are damaged in RAID 5
  - 3 drives are damaged in RAID 6

  The drives in the above configurations are read-only. It is recommended to re-create new drive configuration in such case.

5.4.2 RAID Management Tool

*This function is not supported on VS-101, VS-201, NVR-104.

RAID management tool allows you to carry out capacity expansion, RAID migration, or spare drive configuration with the original drive data reserved.



- Expand capacity

  This function enables drive capacity expansion by replacing the drives in a configuration one by one. This option is supported for the following drive configurations:

  - RAID 1 expansion
  - RAID 5 expansion
  - RAID 6 expansion

- Add hard drive

  This function enables adding new drive member to a drive configuration. It is supported for the following drive configurations:

  - RAID 5 expansion

- Migrate

  This function enables a drive configuration to be migrated to a different RAID configuration. It is supported for the following drive configurations:

  - Migrate single drive to RAID 1, 5, or 6
  - Migrate RAID 1 to RAID 5 or 6
  - Migrate RAID 5 to RAID 6

- Configure spare drive

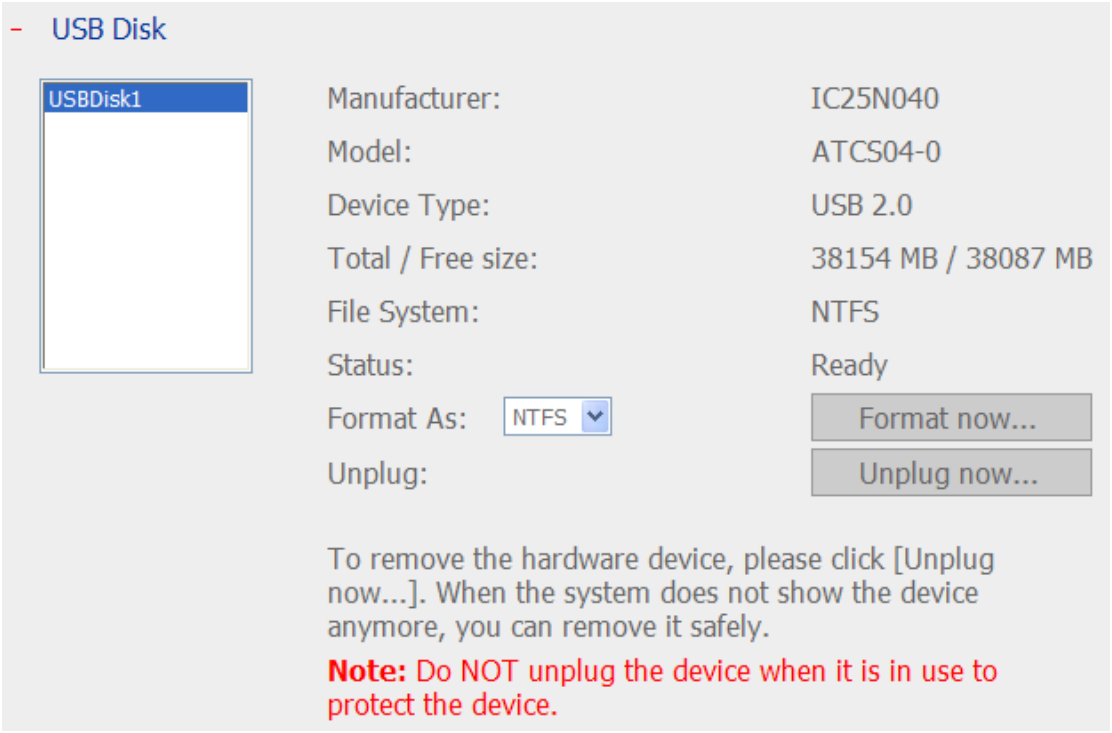
This function enables adding or removing RAID 5 spare drive. The options available are:

- Add spare drive in RAID 5
- Remove spare drive in RAID 5

For detailed operation, please click “Comment” on the management interface to view the detailed operation instructions.

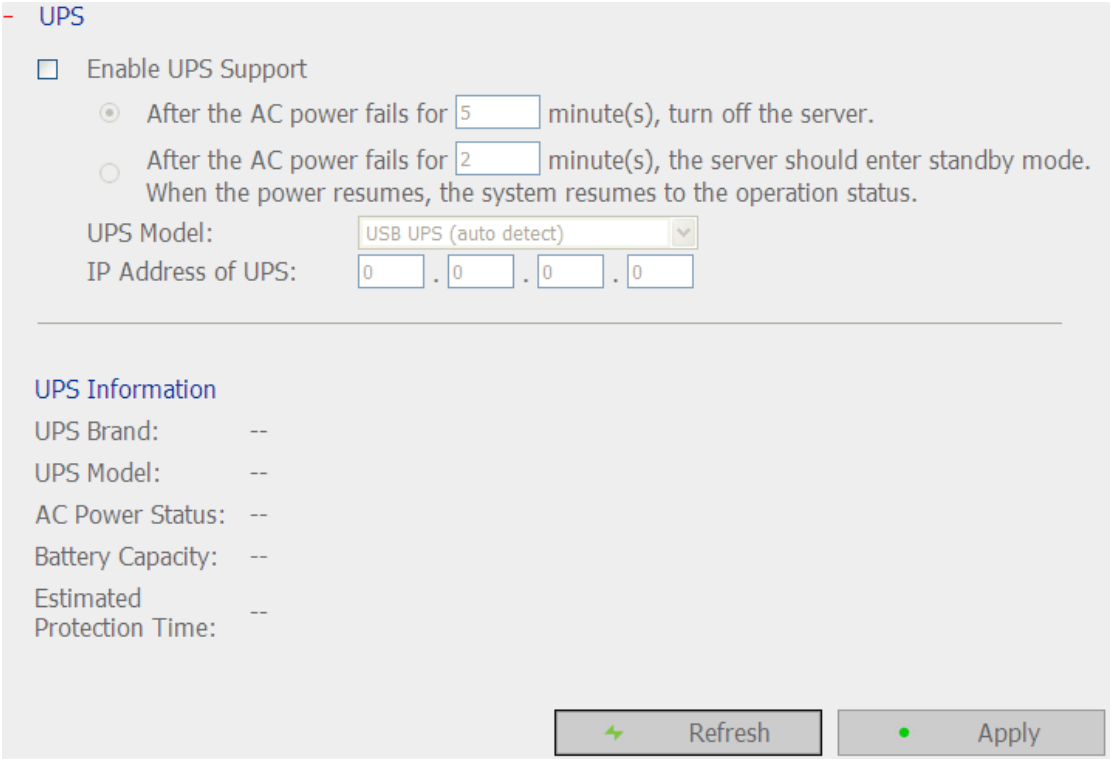
5.4.3 USB Disk

The VioStor supports USB disks for backup storage. Connect the USB device to the USB port of the server, when the device is successfully detected, the details are shown on this page.



5.4.4 UPS

If there is UPS, you can enable UPS support. If the AC power is abnormal, the system will shut down according to the settings. If the time has not reached and the power of the UPS is not sufficient, the system will shut down immediately to protect the server.



* It is recommended to connect UPS to one of the USB ports at the back of server.

- **Enable UPS Support**

  Check this option to enable UPS support. You can configure the time when the system should shut down when AC power status is abnormal. In general, UPS can supply power for 5-10 minutes when AC power is down depending on the maximum load and number of connected devices of the UPS.

- **UPS Model**

  Select the UPS model on the list. If your UPS is not available on the list, please contact the distributor or the technical support of QNAP.

- **IP Address of UPS**

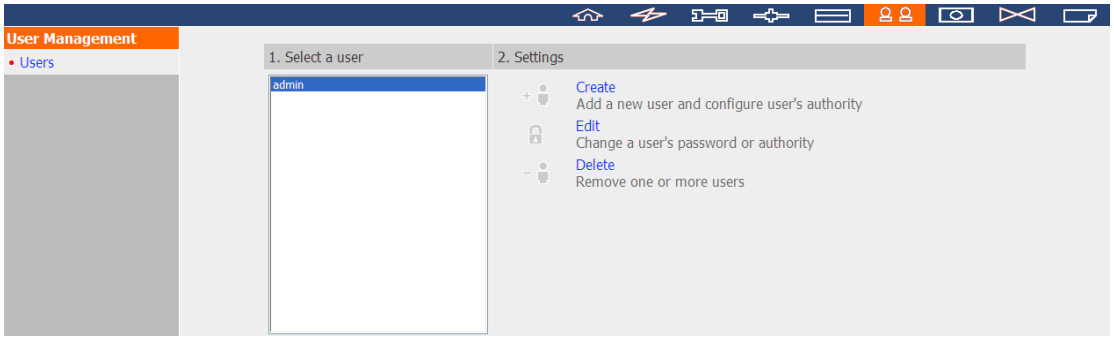
  If you select "APC UPS with SNMP Management", please enter the IP address of the UPS.

  Note: It is recommended to use APC Smart-UPS 700+ APC Network Management Card.

5.5 User Management

The server can be accessed by multiple users. For easier management and better control of users' access right, you have to organize users, user groups and their access right control.

Note: The server supports up to 32 users (including system default users). You can create new users when necessary.



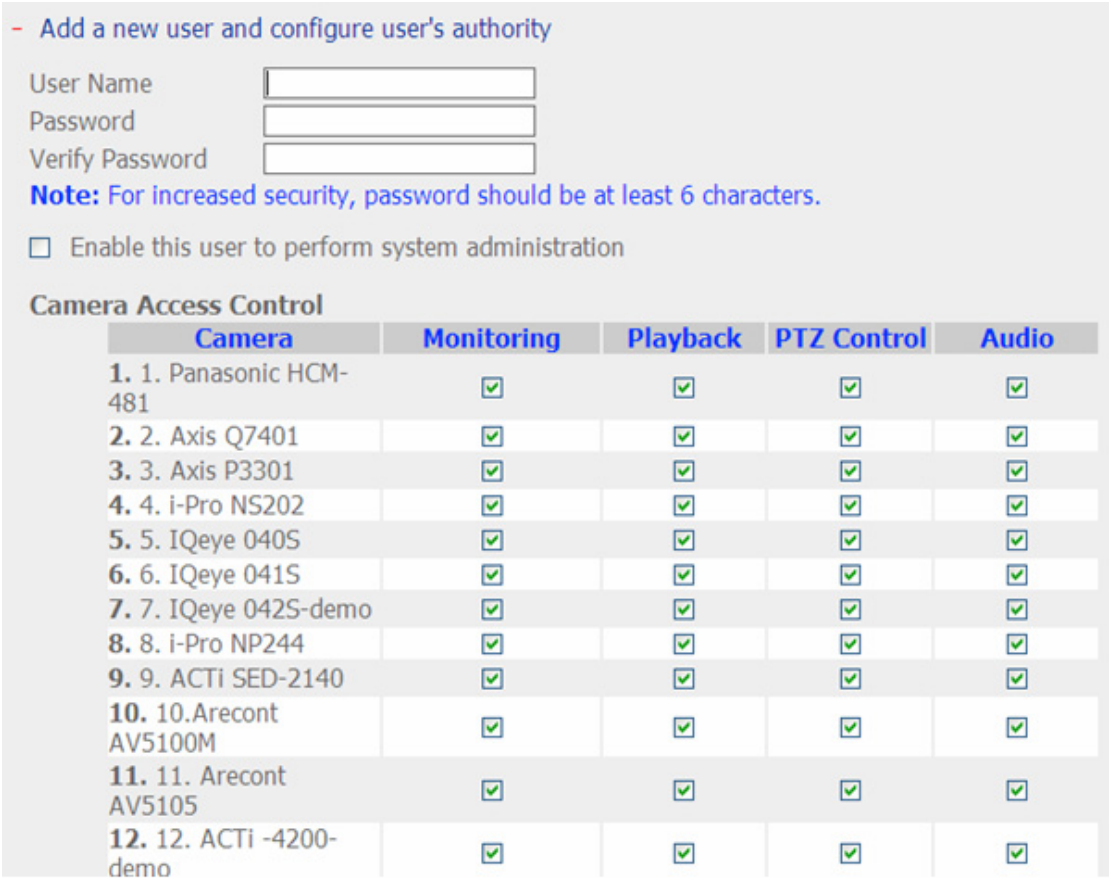
There are two types of users:

- Administrators (admin)
  By default, the administrator has access to system administration and cannot be deleted. Newly created user with system administration right can be deleted.
- User
  User has monitoring right only but cannot enter administration page.

You can perform the following actions for user management:

1. Create user
2. Edit user
3. Delete user

5.5.1 Create user



- **User Name**

  The user name cannot be pure number. It must not exceed 32 characters. It is case-insensitive and supports double-byte characters, such as Chinese, Japanese, and Korean except:

  " / \ [ ] : ; | = , + * ? < > ` '

- **Password**

  The password is case-sensitive and can be 16 characters long at maximum. It is recommended to use a password of at least 6 characters.

- **Enable this user to perform system administration**

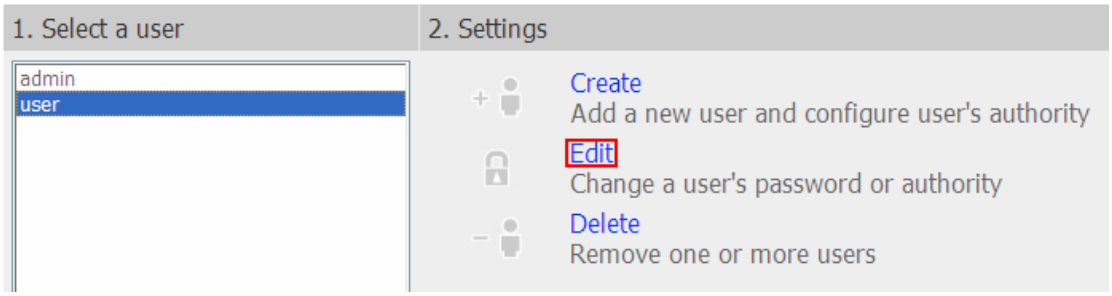
  Assign administration right to the user.

- **Camera Access Control**

  Enable user to monitor the camera or playback the recording.

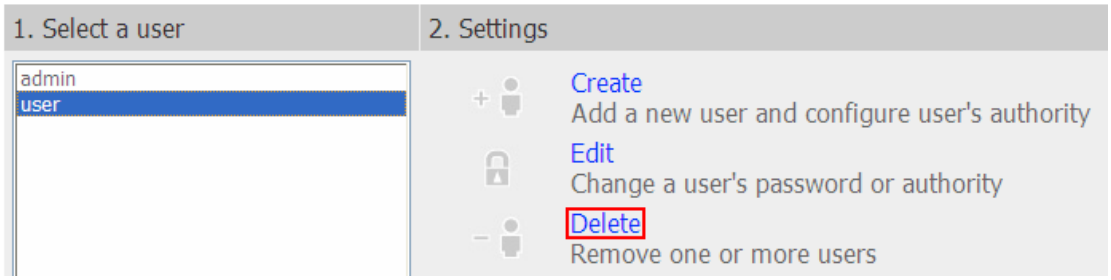
5.5.2 Edit User

Select a user on the list and click "Edit". You can change the password; assign system administration and camera access control. However, the user name cannot be changed.



5.5.3 Delete User

To delete a user, select a user on the list and click "Delete". Click "OK" to confirm.



Note: The system administrator (admin) cannot be deleted.

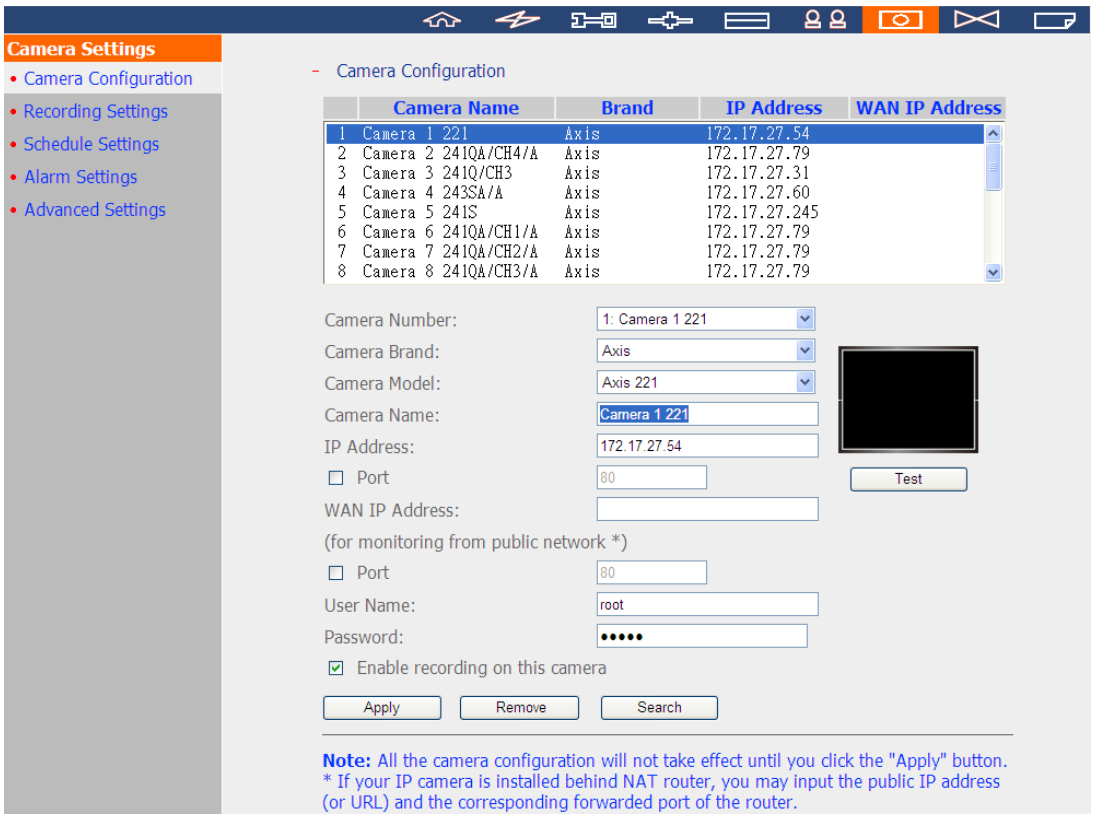
5.6 Camera Settings

You can configure network camera, recording, schedule, alarm, and advanced settings.

5.6.1 Camera Configuration

Please follow the steps below to configure the network cameras.

1. Select a camera number.
2. Select the camera brand.
3. Select the camera model.
4. Enter the camera name.
5. Enter the IP address or domain name of the camera.
6. Enter the user name and password to login the camera.
7. Select to enable recording or not.
8. Click "Apply" to save the settings.



Note:

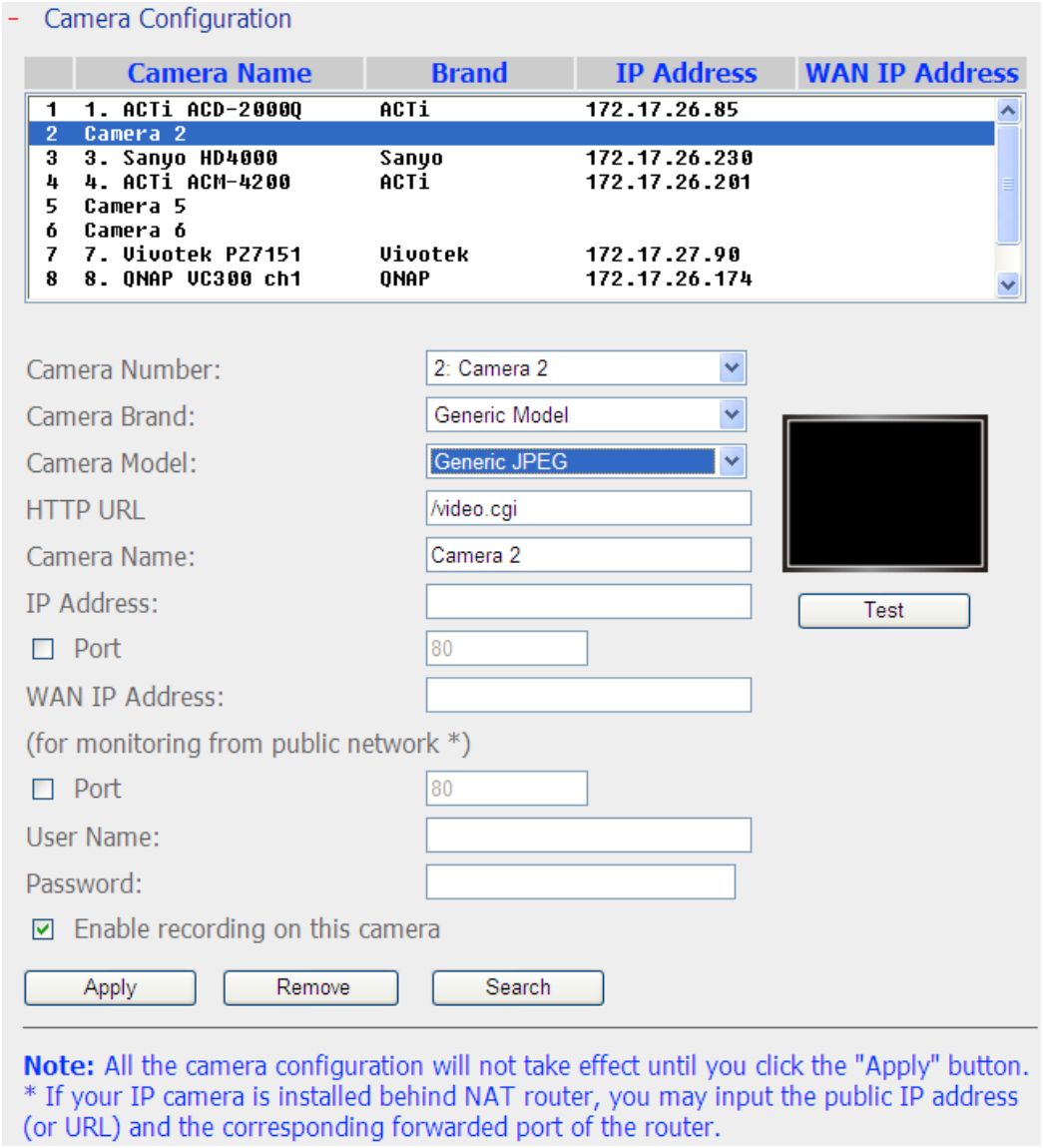
1. All the settings will not take effect until you click "Apply". When applying the changes, recording operation will stop for a while (maximum 1 minute) and then restart.
2. Click "Search" to search for the IP cameras in the local network. Select a channel for the camera and click "Add" to add the camera. By using the search function, the camera model and the IP address are filled in automatically. Click "Close" to close the search results.

Add generic IP camera support by CGI command

QNAP NVR provides an interface for the users to enter the JPEG CGI command of IP cameras in order to receive the video and audio streaming data from the IP cameras and monitor, record, and playback the video of the IP cameras on the NVR. This feature largely enhances the compatibility and expandability of the NVR.

Please follow the steps below to configure your IP camera.

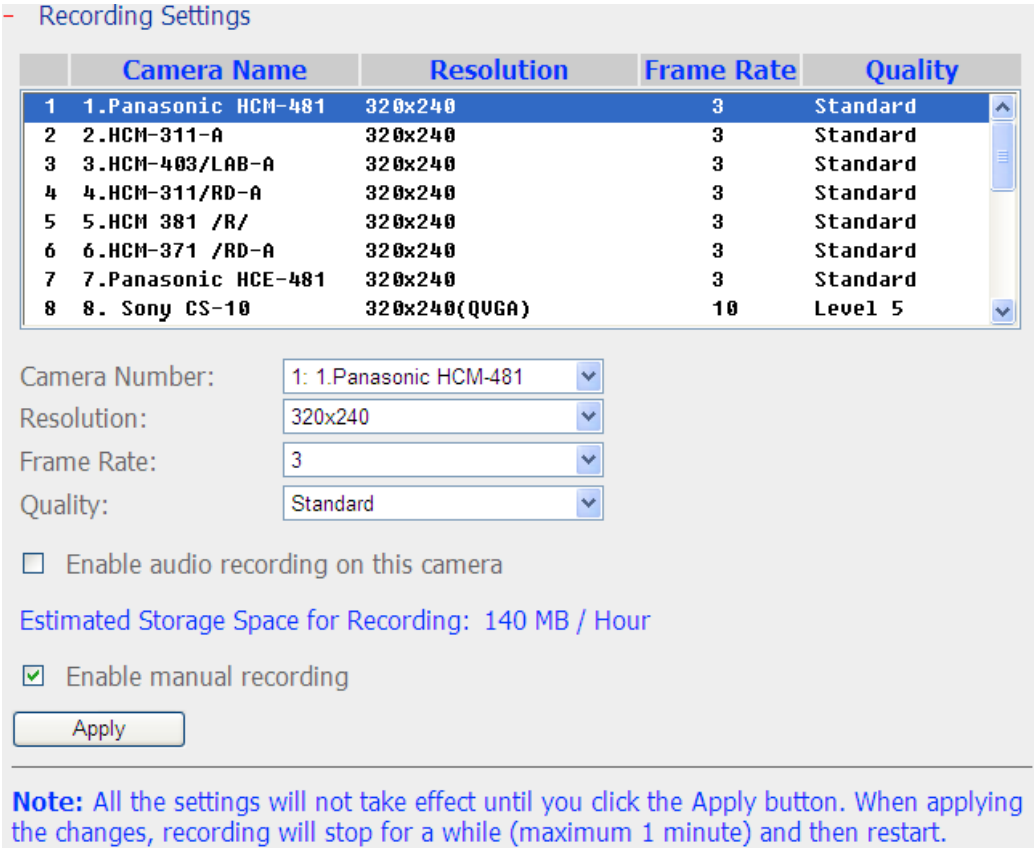
1. Select the IP camera number.
2. Select "Generic Model" for the camera brand.
3. Select "Generic JPEG" for camera model.
4. Enter the cgi path of the IP camera in "HTTP URL" field.
5. Enter the camera name or the IP address of the camera.
6. Enter the user name and password for the IP camera.
7. Select to enable recording or not.
8. Click "Apply" to save the settings.



Note: QNAP NVR only supports JPEG CGI command interface, but does not guarantee the compatibility with all IP camera brands.

5.6.2 Recording Settings

Select a camera on the list and configure the recording resolution, frame rate, and quality. You can also enable manual recording. Click "Apply" to save the settings.



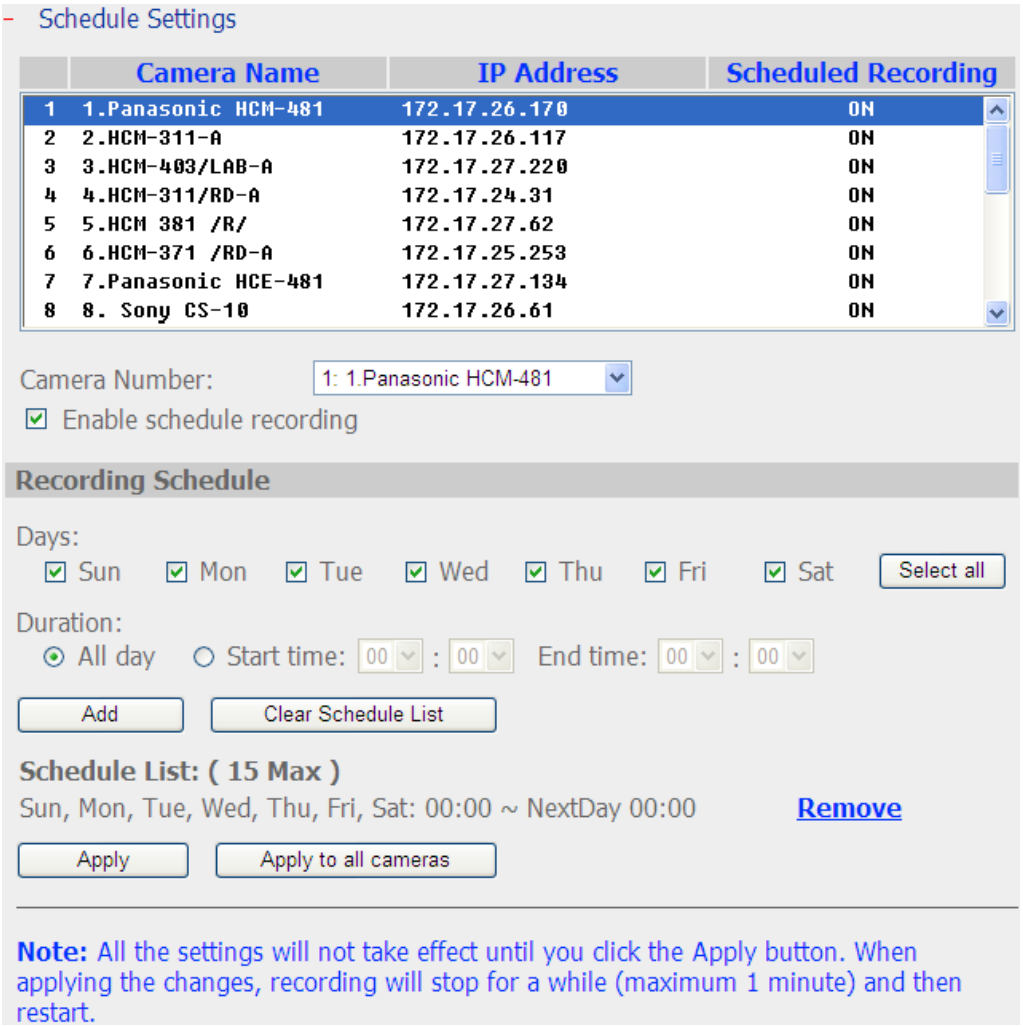
1. **Resolution:** Select the recording resolution.
2. **Frame rate:** Adjust the frame rate for recording. Note that the frame rate of the camera may be affected by the traffic of the network.
3. **Quality:** Select the image quality for recording. Higher quality consumes more disk space.
4. **(Option) Audio recording:** To enable audio recording, click Enable audio recording on this camera.
5. **Estimated storage space for recording:** The number of estimated storage space for recording is only for reference. The actual space consumed depends on the network environment and camera performance.
6. **Manual recording:** To allow manual activation and deactivation of manual recording function on monitoring page, enable this option.

Note:

- Starting and stopping manual recording will not influent scheduled or alarm recording tasks. They are independent processes.
- All the settings will not take effect until you click "Apply". When applying changes, recording operation will stop for a while (maximum 1 minute) and then restart.

5.6.3 Schedule Settings

You can select continuous recording or scheduled recording. The default setting is continuous recording. To set up a recording schedule, please select a camera number on the list. Then select the date and time and click "Add". Click "Apply" to save the settings for the camera or click "Apply to all cameras" to apply to settings to all the cameras. To delete a schedule, click "Remove" on the schedule list.



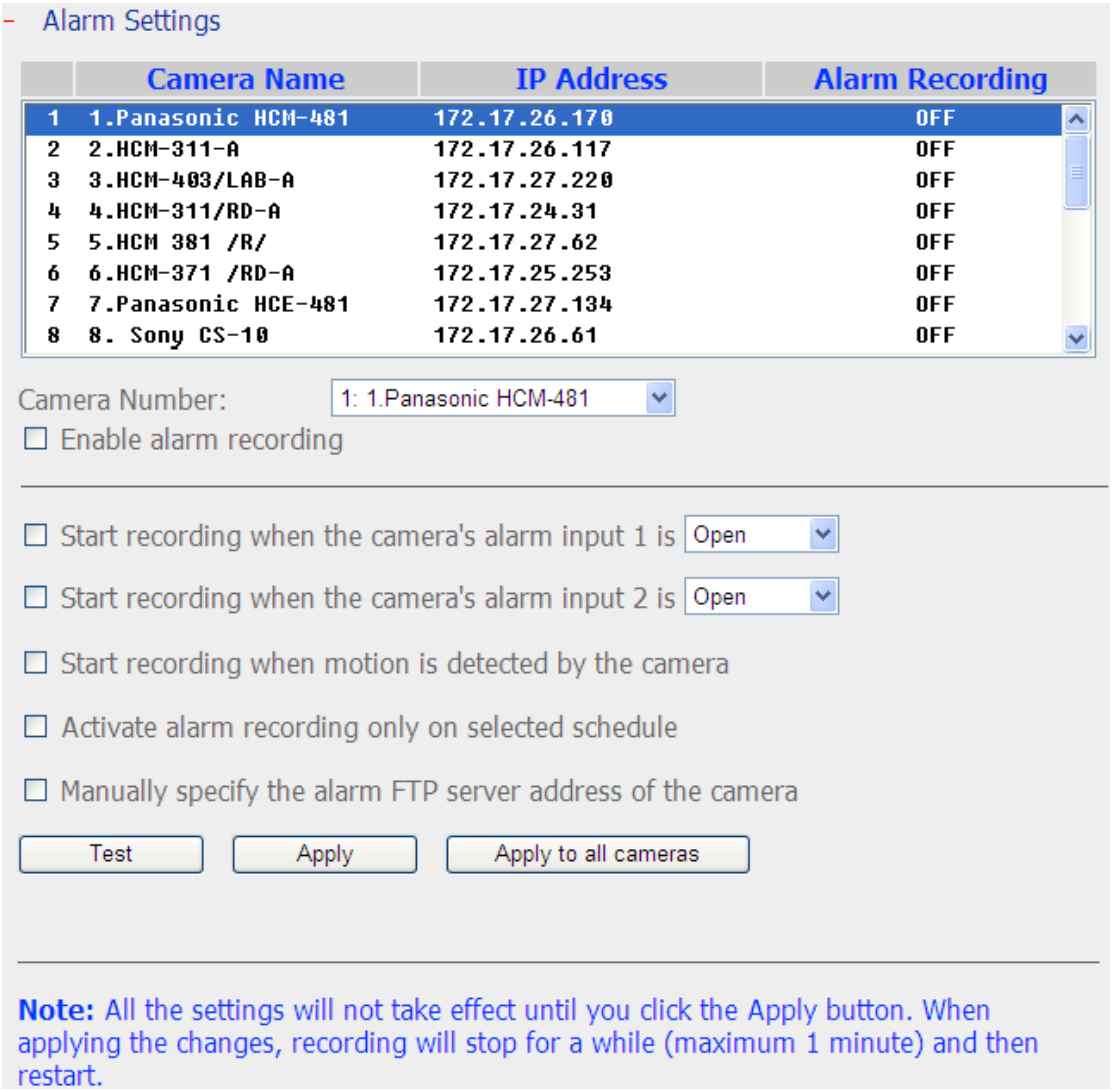
Note:

1. You can add up to 15 schedules.
2. All the settings will not take effect until you click "Apply". When applying changes, recording operation will stop for a while (maximum 1 minute) and then restart.

5.6.4 Alarm Settings

You can enable alarm recording of the cameras. The recording will be triggered by alarm input of the camera or motion detected by the camera.

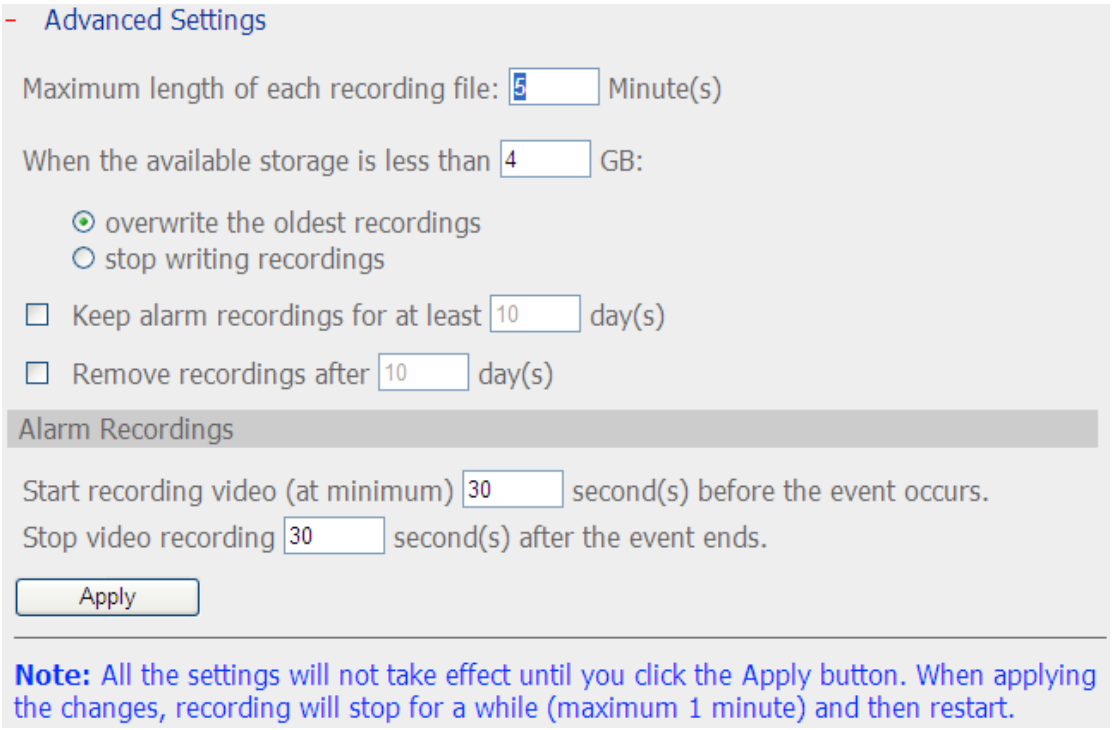
When you enable the option "Activate alarm recording only on selected schedule", alarm recording will be activated only when alarm input is triggered or motion is detected within the preset schedule. You could test the camera setting by clicking "Test". Click "Apply" to save the settings for the camera or click "Apply to all cameras" to apply to settings to all the cameras.



Note: All the settings will not take effect until you click "Apply". When applying changes, recording operation will stop for a while (maximum 1 minute) and then restart.

5.6.5 Advanced Settings

You can configure advanced recording settings in this section.



- **Maximum period for each recording file:** Configure the maximum length of each recording file (maximum 15 min).

- **When the available storage is less than...GB:** Select the action to take when the available storage is less than the preset level. You can select to overwrite the oldest recordings or stop writing new recordings.

- **Keep alarm recordings for at least...day(s):** Specify the number of days that alarm recordings will be retained. This will prevent the recording files from being overwritten when the free storage space is insufficient.

- **Remove recordings after...day(s):** Enter the number of calendar days for VioStor to keep the recording files.
  Please make sure your storage capacity is enough for saving the data for the number of calendar days you set. When recording data has reached the expiry date, expired video files will be deleted. For example, if you set to delete recording data after 7 calendar days, on the 8th day, files recorded on the first day of each camera will be deleted so that VioStor can start to save data of the 8th day.

- Pre/Post Alarm Recordings
  - **Start recording video…second(s) before the event occurs:** Enter the number of seconds to start recording before an event occurs.
  - **Stop video recording…second(s) after the event ends:** Enter the number of seconds to stop recording after an event ends.

  The maximum number of seconds for the above settings is 300, i.e. 5 minutes.

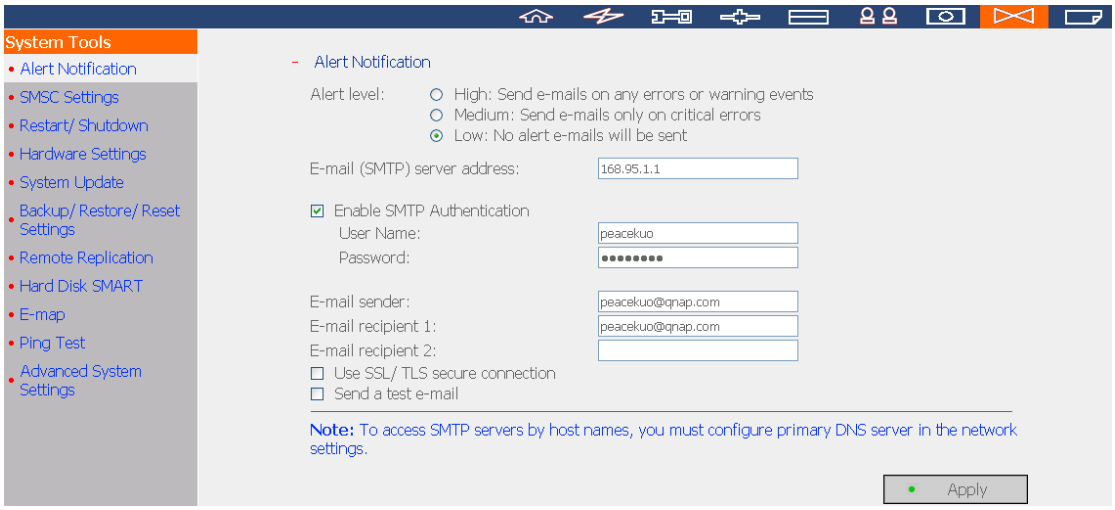
Note: All the settings will not take effect until you click "Apply". When applying changes, recording operation will stop for a while (maximum 1 minute) and then restart.

5.7 System Tools

System Tools enable you to optimize the system maintenance and management. You can set alert notification, restart or shut down the server, configure hardware settings, system update, back up/ restore/ reset settings, set E-map and do ping test.

5.7.1 Alert Notification

Enter the e-mail address of the administrator and the IP address of the SMTP server. In case of warning or malfunction, e.g. power outage, a drive is unplugged, an e-mail will be sent to the administrator automatically. You can go to Event Logs to check the details of all errors and warnings.



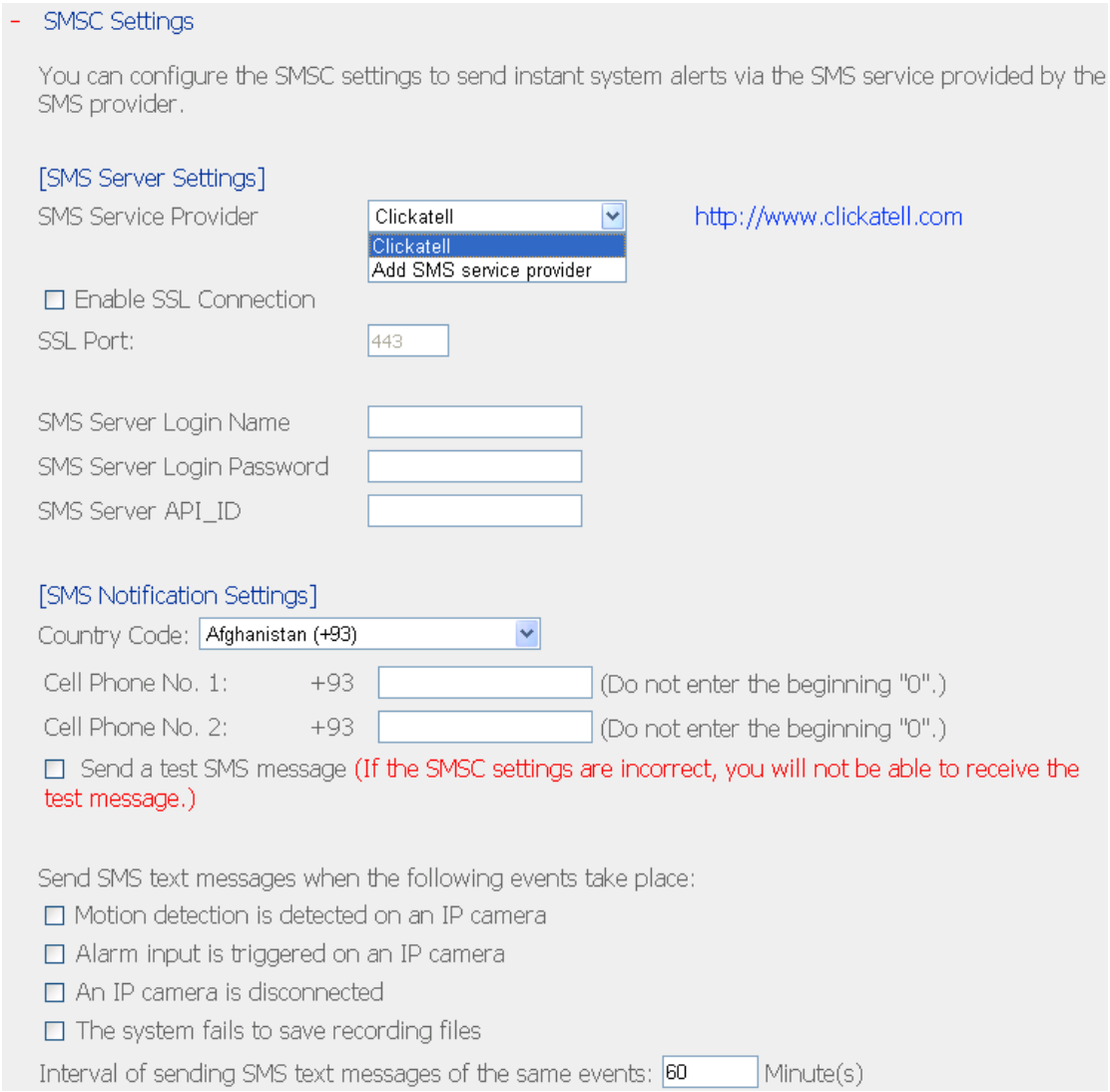
Note: It is recommended to send a test e-mail to make sure you can receive the alert mails.

5.7.2 SMSC Settings

You can configure the SMSC (Short message service center) settings to send SMS text messages to particular mobile phone numbers when an event takes place on the NVR. The default SMS service provider is Clickatell. You may also add your own SMS service provider by selecting "Add SMS Provider" on the drop down menu.

When you select "Add SMS service provider", you need to enter the name of the SMS provider and the URL template text.

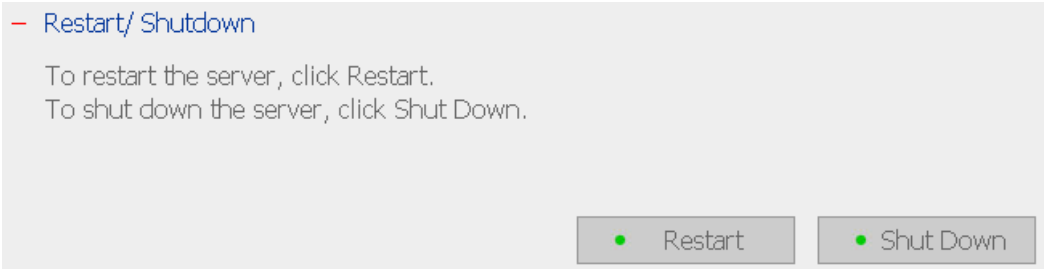
Note: You will not be able to receive the SMS properly if the URL template text entered does not follow your SMS service provider's standard.



5.7.3 Restart/ Shut Down

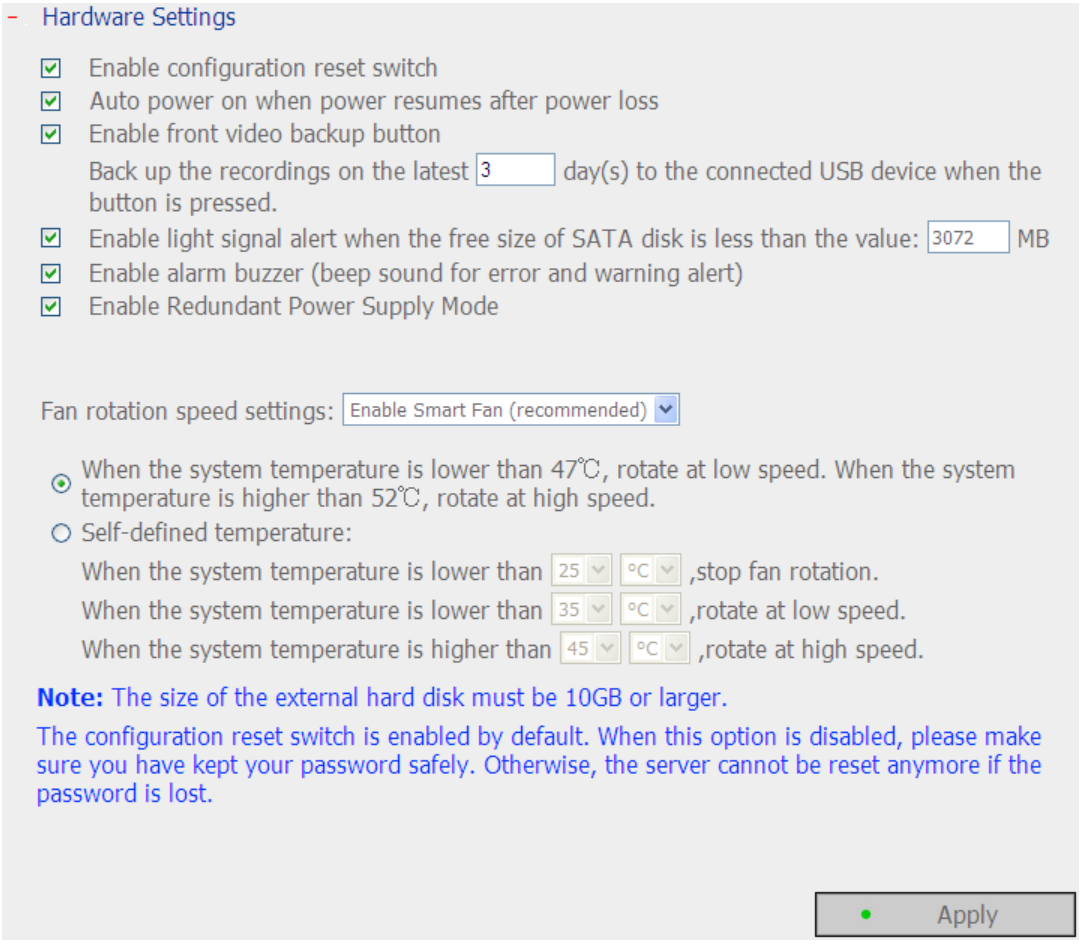
Follow the steps below to restart or shut down the server.

1. Go to “System Tools” > “Restart/ Shutdown”.
2. Click “Restart” to reboot the server or “Shut Down” to turn off the server.



5.7.4 Hardware Settings

You can enable or disable the hardware functions of the server.



- **Enable configuration reset switch**

  By enabling this option, you can press the reset button for 5 seconds to reset the administrator password and system settings to default.

  Note: The configuration reset switch is enabled by default. When this option is disabled, please make sure you have kept your password safely. Otherwise, the server cannot be reset anymore if the password is lost.

- **Auto power on when power resumes after power loss**

  When this function is enabled, the server will turn on automatically when the power resumes after power loss.

- **Enable front video backup button**

  VioStor supports direct copy of recording data on the server to the connected USB device via the USB port. You can set the number of days that the video is recorded to copy to the device. To use this function, please follow the steps below:

  1. Set the number of days that the latest recordings should be backed up. If 3 days are entered, the recordings of today, yesterday and the day before yesterday will be backed up.
  2. Connect a USB storage device, e.g. USB disk drive to the front USB port of VioStor.
  3. Press and hold the one touch auto video backup button for 3 seconds*. The recording data on NVR will start to be copied to the USB device instantly. If the USB device is recognized, the USB LED glows in blue. The USB LED will blink in blue when the data is being copied. The LED will become blue again when data copy is finished. You can then safely remove the device.

     Note: Video backup function supports only USB device of 10GB storage capacity or above.
     This function is not supported on VS-8040U-RP, VS-8032U-RP, VS-8024U-RP.

     * If you are using VS-101/ VS-201/ NVR-104, please press the button for 0.5 second to execute data copy.

- **Enable light signal alert when the free size of SATA disk is less than the value**

  The status LED flashes red and green when this function is enabled and the free space of the SATA disk is less than the value. The range of the value is 1-51200 MB.

- **Enable alarm buzzer**

  Enable this option. The system will sound when an error occurs.

- **Enable Redundant Power Supply Mode**

  When the redundant power supply mode is enabled, the server beeps if any of the power supply units does not function properly.

  *This function applies to the models with redundant power supply only.

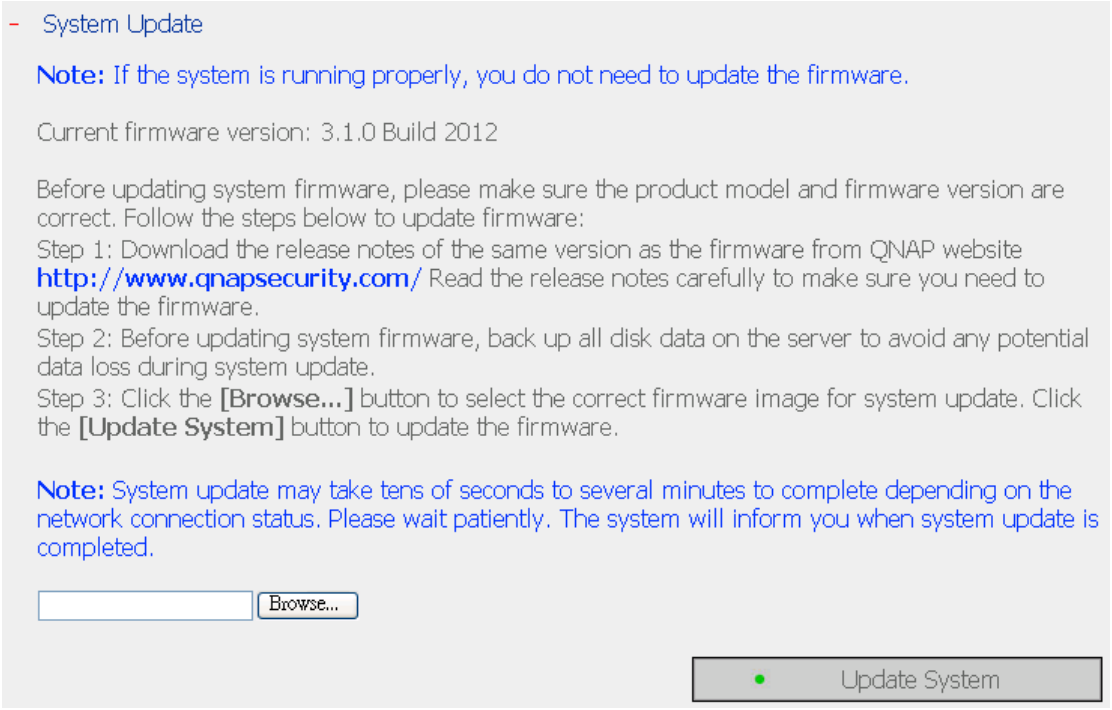
- **Smart Fan configuration**

  After enabling the smart fan, the fan rotation speed is automatically adjusted according to the server temperature. It is recommended to enable this option. By manually setting the fan rotation speed, the fan rotates at the defined speed continuously.

  *This function is not supported on VS-101, VS-201, NVR-104.

5.7.5 System Update

Before updating the system firmware, please make sure the product model and the firmware version are correct. Follow the steps below to update firmware:



1. Download the release notes of the same version as the firmware from QNAP website http://www.qnapsecurity.com/. Read the release notes carefully to make sure you need to upgrade the firmware.
2. Before upgrading the system firmware, back up all disk data on the server to avoid any potential data loss during system update.
3. Click "Browse…" to select the correct firmware image. Click "Update System" to update the firmware.

The system update may take several minutes to complete depending on the network connection status. Please wait patiently. The system will inform you when system update is completed.

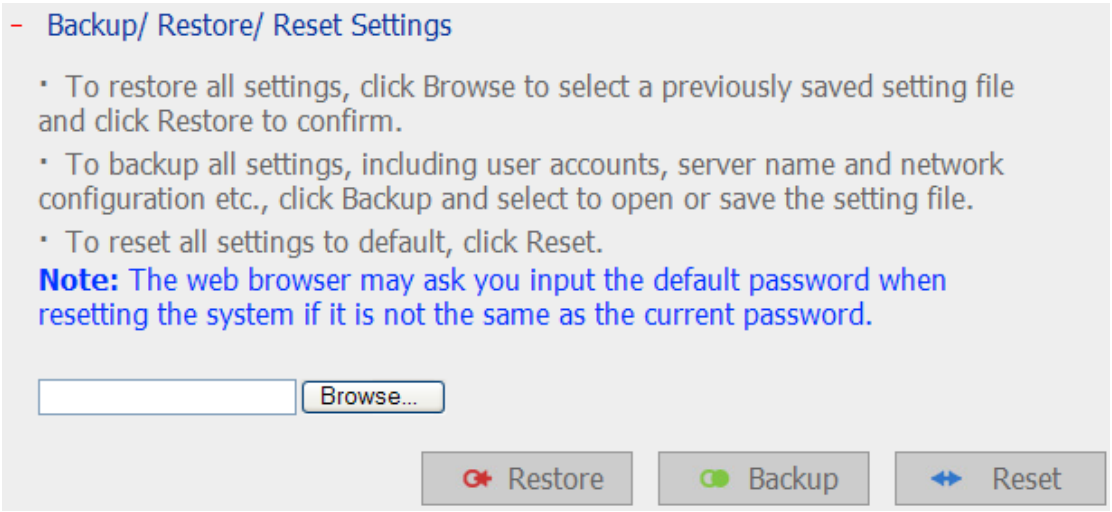
When performing system update, please make sure the power supply is at a steady state. Otherwise, the system may be unable to start up.

Note: If the system is running properly, you do not need to update the firmware. QNAP is not responsible for any forms of data loss caused by improper or illegal system update.

5.7.6 Backup/ Restore/ Reset Settings

- To backup all the settings, including user accounts, server name and network configuration etc., click "Backup" and select to open or save the setting file.
- To restore all settings, click "Browse" to select a previously saved setting file and click "Restore" to confirm.
- To reset all settings to default, click "Reset". All data on the disk(s) will be deleted.

Caution: When you press "Reset" on this page, all the drive data, user accounts, network shares, and system settings are cleared and restored to default. Please make sure you have backed up all the important data and system settings before resetting the NVR.

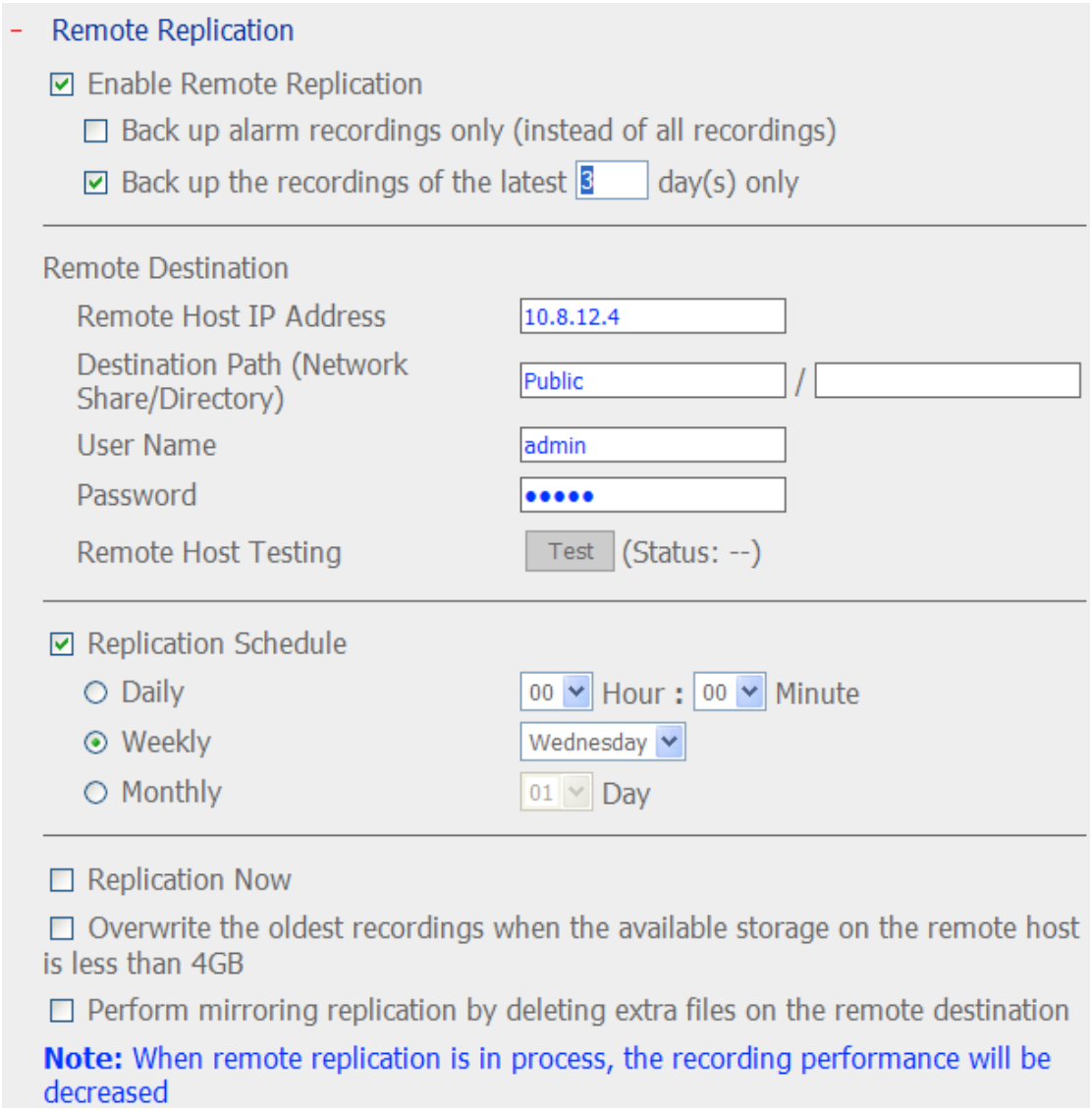


5.7.7 Remote Replication

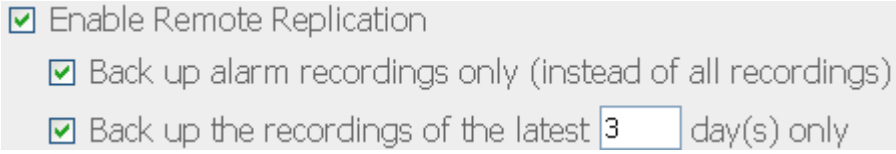
You can use the remote replication feature to copy the recording data of the local VioStor to a remote QNAP network attached storage (TS-509). The remote QNAP NAS is hereafter referred to as "the remote storage device".

Note: Before using this function, please make sure the Microsoft networking service of the remote storage device is enabled, and the corresponding path and user access right have been correctly configured.

1. Login VioStor and enter "System Tools" > "Remote Replication".



2. Enable remote replication (support multiple choices)



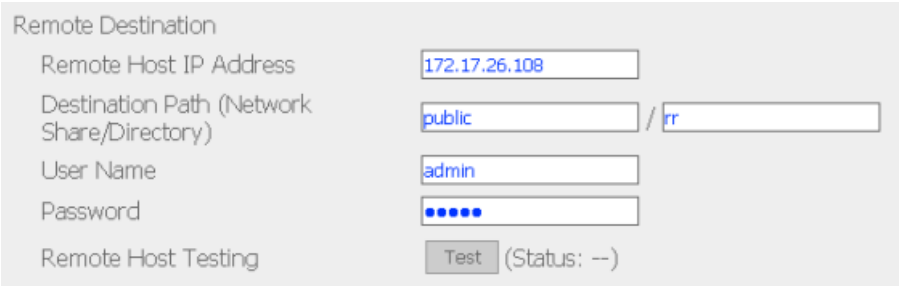
In the above example, the system only copies the alarm recording data of the latest 3 days to the remote storage device.

- Check the box "Enable remote replication" to activate this feature. The system executes automatic backup of recording data to the remote storage device according to the settings.

- When you select "Back up alarm recordings only (instead of all recordings)", the system will only copy alarm recording data to the remote storage device. If this option is unchecked, the system will backup all recording data to the remote storage device.

- When you select "Back up the recordings of the latest…day(s) only" and enter the number of days, the system will back up the latest recording data to the remote storage device automatically according to your settings. If this option is unchecked, the system will copy all recording data to the remote storage device.

3. Configure your remote storage server

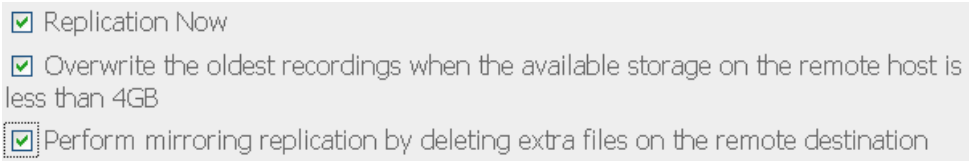


Note: It is recommended to execute the "Remote host testing" function to verify the connection to the remote storage device is successful.

4. Configure the remote replication schedule

For example, to enable the system to copy recording data automatically to remote storage device at 01:15 every Monday, please do the following:
Check the box "Replication Schedule", select "Weekly", enter 01 Hour: 15 minute, and select "Monday".

5. Backup Options



- Select "Replication Now", the system backs up recording data to remote storage device immediately.

- Select "Overwrite the oldest recordings when the available storage on the remote host is less than 4GB"; the system overwrites the oldest recording data when the free space on the server is less than 4GB.

- Select "Perform mirroring replication by deleting extra files on the remote replication", the system syncs the recording data between VioStor and the remote storage device and delete any extra files on the remote destination.

- When the above options are all checked, the system executes remote replication immediately. It first judges if there are extra files on the remote location that are different from the local source. If yes, the extra files will be removed. After that, the system executes recording data backup and verifies if the free space of the internal hard disk drive is less than 4GB. If the free storage capacity is larger than 4GB, remote replication will be executed immediately. If the free storage space is less than 4GB, the system deletes the recording data of the oldest day and executes remote replication.

- The system displays the latest 10 remote replication records for you to analyze the status and troubleshooting.

Start Time	Finish Time	Replicated Data Size	Status
2007-11-08 18:00:07	2007-11-09 06:29:39	54.36 GByte(s)	Succeeded
2007-11-07 18:00:06	2007-11-08 10:18:26	74.17 GByte(s)	Succeeded
2007-11-06 18:00:02	2007-11-06 19:56:31	12.24 GByte(s)	Succeeded
2007-11-05 18:00:06	2007-11-05 20:05:06	12.53 GByte(s)	Succeeded
2007-11-04 18:00:03	2007-11-04 19:59:28	11.33 GByte(s)	Succeeded
2007-11-03 18:00:08	2007-11-03 20:01:54	11.75 GByte(s)	Succeeded
2007-11-02 18:14:09	2007-11-02 19:11:16	4.98 GByte(s)	Failed (Remote access error)
2007-11-01 18:00:04	2007-11-02 02:32:27	43.68 GByte(s)	Succeeded
2007-10-31 18:00:05	2007-11-01 03:34:13	33.01 GByte(s)	Failed (An internal error occurred)

In the above example:

1. When the status is shown as "Failed (Remote access error)": You can check the remote storage device is running or the network settings are correct.
2. When the status is shown as "Failed (An internal error occurred)": You can check the hard drive status of VioStor or check the Event Logs.

Note: The time required by VioStor to replicate data to remote storage device varies to the network environment. If the remote replication time is too long, some recording files may be overwritten by the system. To avoid this, it is recommended to refer to the status messages to analyze the time needed for remote replication and adjust the replication schedule accordingly.

5.7.8 Hard Disk SMART

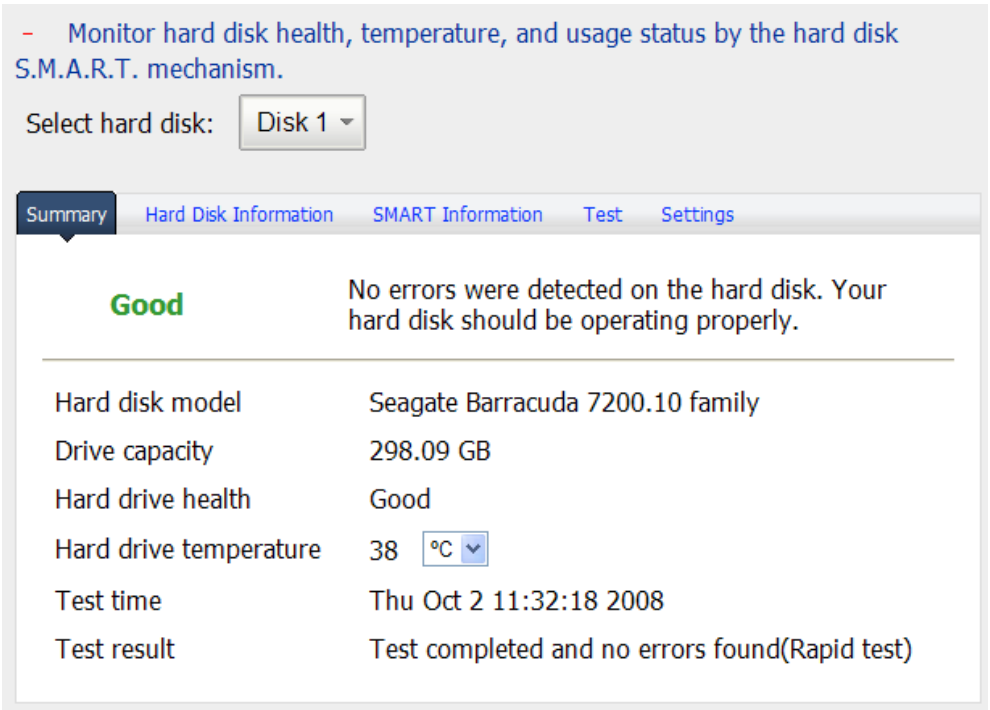
This function is not supported on VS-101, VS-201, NVR-104.

This page enables users to monitor hard drive health, temperature, and usage status by the hard disk S.M.A.R.T. mechanism.

Select the hard drive and you can view the following information by clicking the corresponding buttons.

Field	Description
Summary	Displays the hard drive smart summary and the latest test result.
Hard disk information	Displays the hard drive details, e.g., model, serial number, drive capacity, etc.
SMART information	Displays the hard drive SMART. Any items that the values are lower than the threshold are regarded as abnormal.
Test	To perform quick or complete hard drive SMART test and display the results.
Settings	To configure temperature alarm. When the hard drive temperature is over the preset values, the system records error logs. You can also configure quick and complete test schedule. The latest test result is shown in the Summary page.

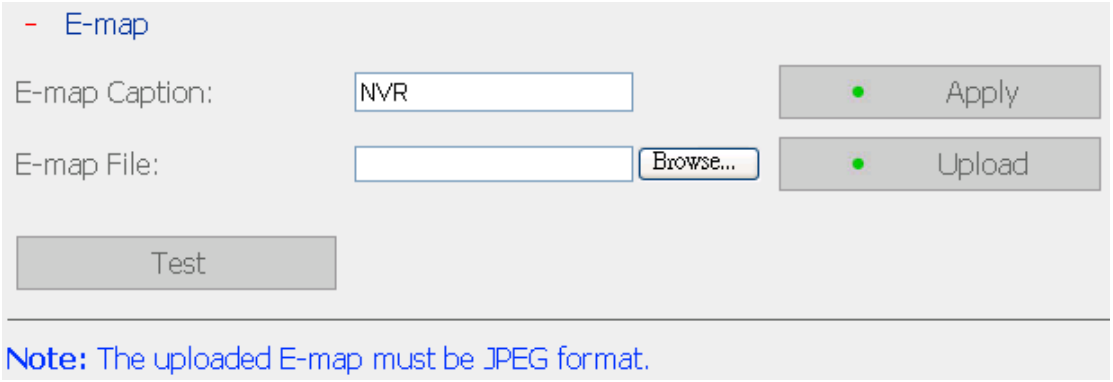
- Monitor hard disk health, temperature, and usage status by the hard disk S.M.A.R.T. mechanism.



5.7.9 E-map

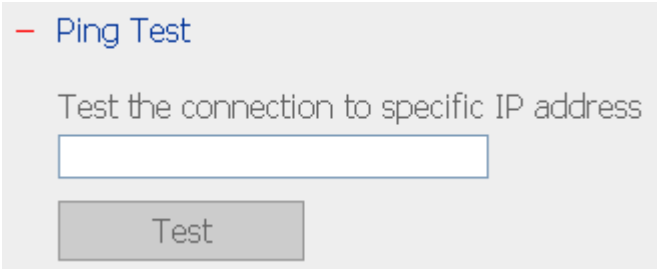
You can upload an E-map to VioStor to illustrate the location of the cameras.

1. To upload an E-map, click "Browse" and select the E-map file. Then click "Upload".
2. You can change the caption for the E-map and click "Apply".
3. After uploading the E-map, click "Test" to view the map.



5.7.10 Ping Test

To test the connection to an IP address, enter the IP address and click "Test".



5.7.11 Advanced System Settings

You can set the timeout period to log off the users from the configuration page when the idling time has reached.

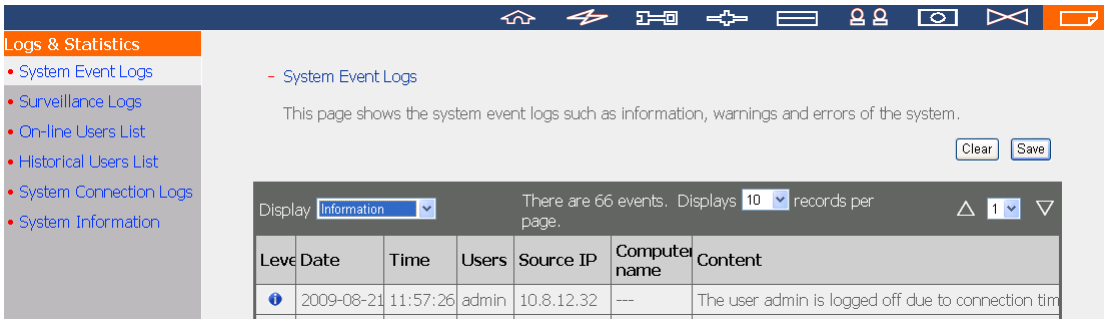
Note: Timeout logoff does not apply to the monitoring, playback, advanced mode, device configuration, system update, remote replication, and Logs & Statistics pages.

5.8 Logs & Statistics

5.8.1 System Event Logs

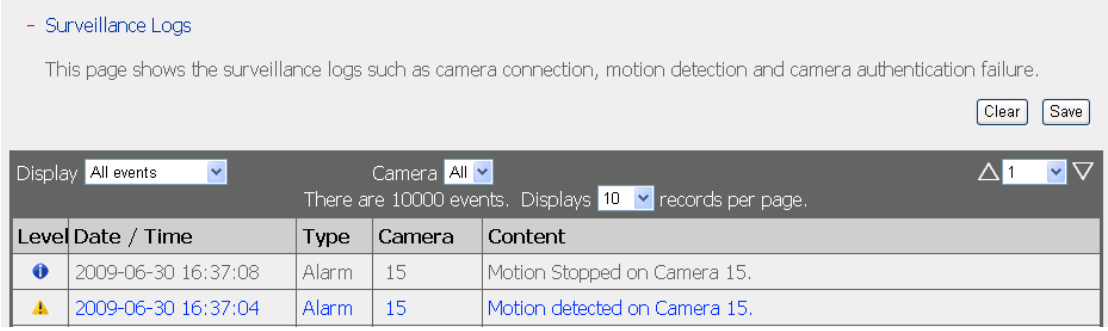
The server can store 10,000 recent event logs, including warning, error, and information messages. In case of system malfunction, event logs (only in English) can be retrieved to analyze system problems.

Click "Save" to save the logs as csv file. Click "Delete" to clear all logs.



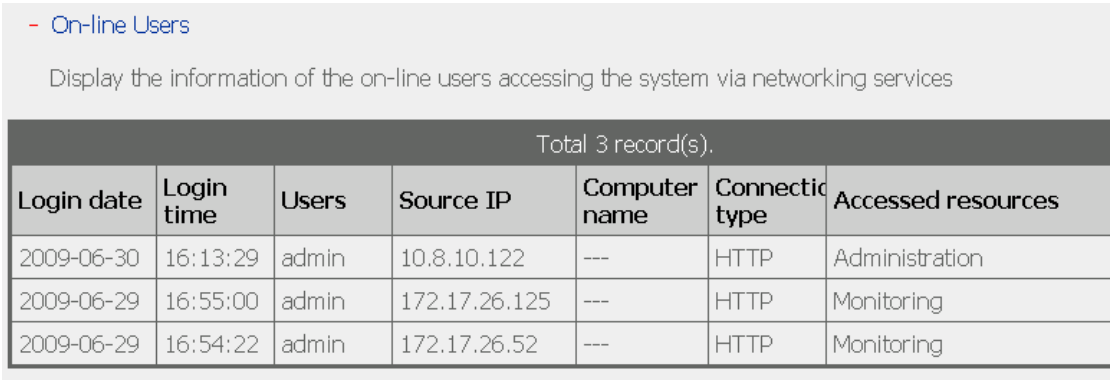
5.8.2 Surveillance Logs

This page shows the surveillance logs such as camera connection, motion detection, and camera authentication failure.



5.8.3 On-line Users List

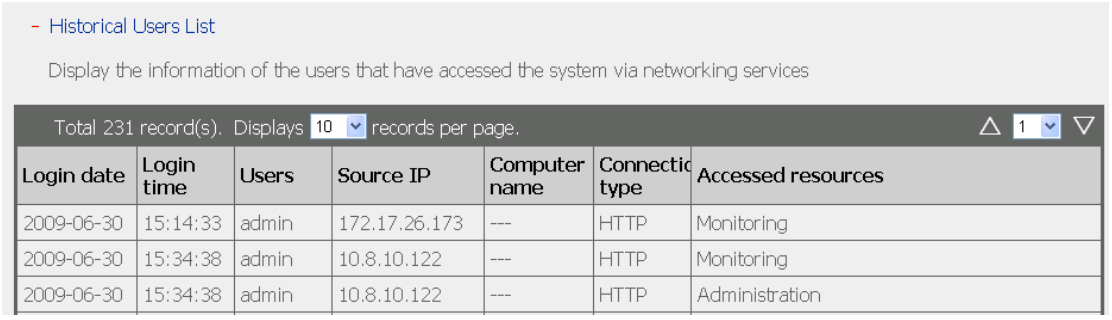
This page shows the information of the currently active users, e.g. the user name, IP address, and login time.



Login date	Login time	Users	Source IP	Computer name	Connectic type	Accessed resources
2009-06-30	16:13:29	admin	10.8.10.122	---	HTTP	Administration
2009-06-29	16:55:00	admin	172.17.26.125	---	HTTP	Monitoring
2009-06-29	16:54:22	admin	172.17.26.52	---	HTTP	Monitoring

5.8.4 Historical Users List

This page shows the information of the users who have logged in the system including the user name, IP address, login time, and the services they have accessed etc.

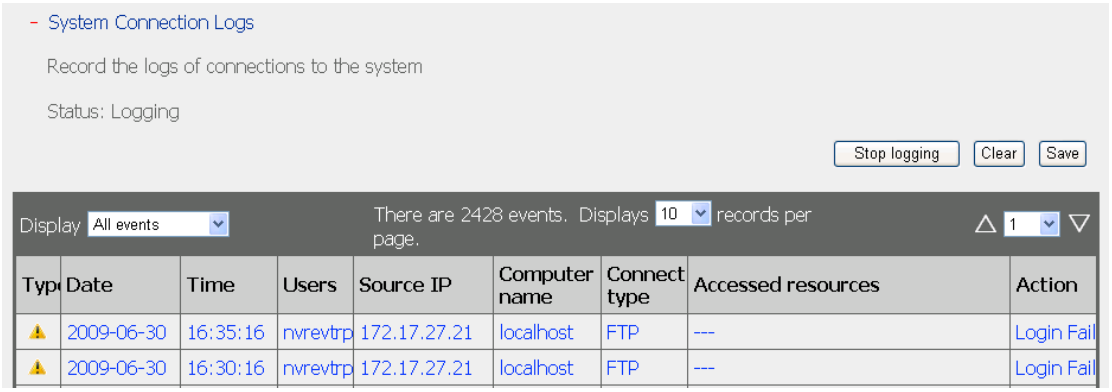


Login date	Login time	Users	Source IP	Computer name	Connectic type	Accessed resources
2009-06-30	15:14:33	admin	172.17.26.173	---	HTTP	Monitoring
2009-06-30	15:34:38	admin	10.8.10.122	---	HTTP	Monitoring
2009-06-30	15:34:38	admin	10.8.10.122	---	HTTP	Administration

5.8.5 System Connection Logs

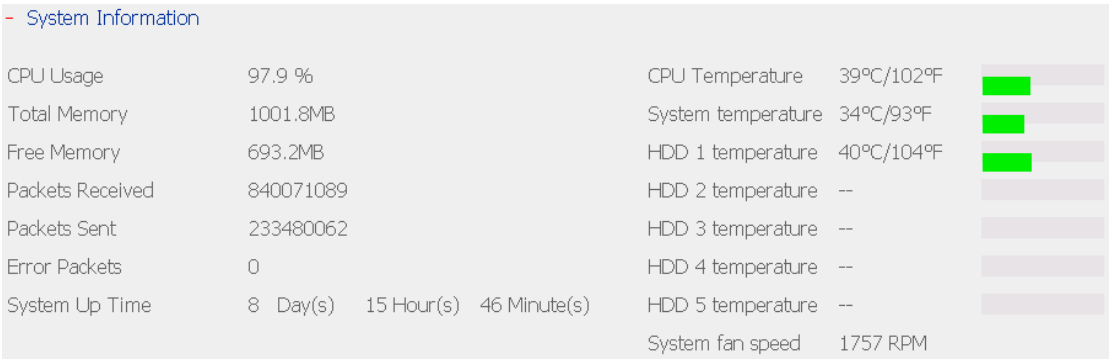
The logs of connections to the server via samba, FTP, AFP, HTTP, HTTPS, Telnet, and SSH are recorded in this page.

You can select to start or stop logging. The file transfer performance can be slightly affected by enabling the event logging.



5.8.6 System Information

This page shows the system information, e.g., CPU usage, memory, and system temperature.



Chapter 6. System Maintenance

This section provides a general overview on system maintenance.

6.1 Reset the Administrator Password and Network Settings

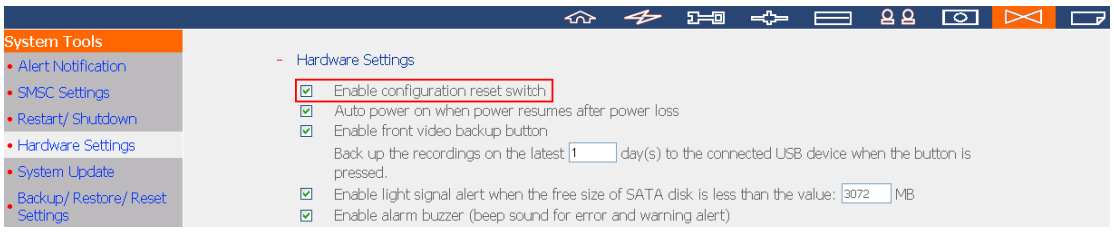
To reset the administrator password and network settings, press the reset button of the server for five seconds. A beep sound will be heard.

After resetting the system, you can login the server with the default user name and password:

Default user name: **admin***
Password: **admin**

*If you are using VS-201/ VS-101/ NVR-104, the login name is 'administrator' and the login password is 'admin'.

Note: To reset the system by the reset button, the option "Enable configuration reset switch" in Hardware Settings must be activated.



6.2 Power Outage or Abnormal Shutdown

In case of power outage or improper shutdown of the server, the server will resume to the state before it is shut down. If your server does not function properly after restart, please do the following:

1. If the system configuration is lost, configure the system again.
2. In the event of abnormal operation of the server, contact customer service for technical support.

To avoid the above situations, please back up your data periodically and make sure you have done the following:

- Follow the instructions described in Chapter 5.7.2 to restart or shut down the server.
- If there is an anticipated power outage, back up all important data and turn off the server properly until power supply is resumed.

6.3 Disk Hot Swapping (RAID Configuration)

This function is not supported on one-bay NVR models.

The VioStor supports hot swapping. When a hard disk of RAID disk volume fails, the failed disk can be replaced by a new one immediately without shutting down the system, and the recording data can be reserved. However, if the hard disks are working properly and recording is in process, do not hot swap the disks to avoid damage to the disks or recording files.

Chapter 7. LCD Panel

* This section is applicable to NVR models with LCD panel only.

The NVR provides a handy LCD panel for you to perform disk configuration and view the system information.

When the NVR is started up, you will be able to view the server name and IP address:

For the first time installation, the LCD panel shows the number of hard drives detected and the IP address. You may select to configure the hard drives.

Number of hard drives detected	Default disk configuration	Available disk configuration options*
1	Single	Single
2	RAID 1	Single -> JBOD ->RAID 0 -> RAID 1
3	RAID 5	Single -> JBOD -> RAID 0 -> RAID 5
4 or above	RAID 5	Single ->JBOD -> RAID 0 -> RAID 5 -> RAID 6

*Press the "Select" button to choose the option, and press the "Enter" button to confirm.

For example, when you turn on the NVR with 5 hard drives installed, the LCD panel shows:

You can press the "Select" button to browse more options, e.g. RAID 6.
Press the "Enter" button and the following message shows. Press the "Select" button to select "Yes" to confirm.

When you execute RAID 1, RAID 5, or RAID 6 configuration, the system will initialize the hard drives, create the RAID device, format the RAID device, and mount it as a volume on the NVR. The progress will be shown on the LCD panel. When it reaches 100%, you can access the RAID volume, e.g. create share folders and upload files to the folders on the NVR. In the meantime, to make sure the stripes and blocks in all the RAID component devices are ready, the NVR will execute RAID synchronization and the progress will be shown on "Disk Management" > "Volume Management" page. The synchronization rate is around 30-60 MB/s (vary by hard drive models, system resource usage, etc.).

Note: If a member drive of the RAID configuration was lost during the synchronization, the RAID device will enter degraded mode. The volume data is still accessible. If you add a new member drive to the device, it will start to rebuild. You can check the status on the "Volume Management" page.

When the configuration is finished, the server name and IP address will be shown. If the NVR fails to create the disk volume, the following message will be shown.

View system information by the LCD panel

When the LCD panel shows the server name and IP address, you may press the "Enter" button to enter the Main Menu. The Main Menu consists of the following items:

1. TCP/IP
2. Physical disk
3. Volume
4. System
5. Shut down
6. Reboot
7. Password
8. Back

1. TCP/ IP

In TCP/ IP, you can view the following options:

- 1.1 LAN IP Address
- 1.2 LAN Subnet Mask
- 1.3 LAN Gateway
- 1.4 LAN PRI. DNS
- 1.5 LAN SEC. DNS
- 1.6 Enter Network Settings
  - 1.6.1 Network Settings – DHCP
  - 1.6.2 Network Settings – Static IP*
  - 1.6.3 Network Settings – BACK
- 1.7 Back to Main Menu

* In Network Settings – Static IP, you can configure the IP address, subnet mask, gateway, and DNS of LAN 1 and LAN 2.

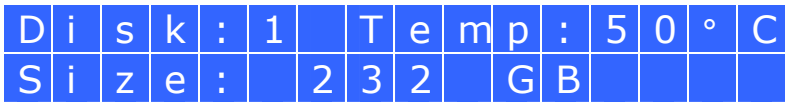
2. Physical disk

In Physical disk, you can view the following options:

2.1 Disk Info

2.2 Back to Main Menu

The disk info shows the temperature and the capacity of the hard drive.



3. Volume

This section shows the disk configuration of the NVR. The first line shows the RAID configuration and storage capacity; the second line shows the member drive number of the configuration.

If there is more than one volume, press the "Select" button to view the information. The following table shows the description of the LCD messages for RAID 5 configuration.

LCD Display	Drive configuration
RAID5+S	RAID5+spare
RAID5 (D)	RAID 5 degraded mode
RAID 5 (B)	RAID 5 rebuilding
RAID 5 (S)	RAID 5 re-synchronizing
RAID 5 (U)	RAID 5 is unmounted
RAID 5 (X)	RAID 5 non-activated

4. System

This section shows the system temperature and the rotation speed of the system fan.

5. Shut down

Use this option to turn off the NVR. Press the "Select" button to select "Yes". Then press the "Enter" button to confirm.

6. Reboot

Use this option to restart the NVR. Press the "Select" button to select "Yes". Then press the "Enter" button to confirm.

7. Password

The default password of the LCD panel is blank. Enter this option to change the password of the LCD panel. Select "Yes" to continue.

You may enter a password of maximum 8 numeric characters (0-9). When the cursor moves to "OK", press the "Enter" button. Verify the password to confirm the changes.

8. Back

Select this option to return to the main menu.

System Messages

When the NVR encounters system error, an error message will be shown on the LCD panel. Press the "Enter" button to view the message. Press the "Enter" button again to view the next message.

System Message	Description
Sys. Fan Failed	The system fan failed
Sys. Overheat	The system overheat
HDD Overheat	The hard drive overheat
CPU Overheat	The CPU overheat
Network Lost	Both LAN 1 and LAN 2 are disconnected in Failover or Load-balancing mode
LAN1 Lost	LAN 1 is disconnected
LAN2 Lost	LAN 2 is disconnected
HDD Failure	The hard drive fails
Vol1 Full	The volume is full
HDD Ejected	The hard drive is ejected
Vol1 Degraded	The volume is in degraded mode
Vol1 Unmounted	The volume is unmounted
Vol1 Nonactivate	The volume is not activated

Chapter 8. Troubleshooting

1. The monitoring screen did not display.

Please check the following:

A. Check if you have installed ActiveX when logging in the monitoring page. Set the security level to "Medium" or lower in Internet Options of IE browser.

B. Make sure VioStor is turned on and the network is correctly connected.

C. The IP address of VioStor does not conflict with other devices in the same subnet.

D. Check the IP address settings of VioStor and your computer. Make sure they are in the same subnet.

2. In the monitoring page, unable to view live video on one of the cameras.

Please check the following:

A. The IP address, name, and password entered in the camera configuration page are correct. You can use the "Test" function to verify the connection.

B. When the PC and the network camera are in the same subnet, while VioStor is in another one, you cannot view the monitoring screen from the PC. You can solve the problems by the following methods:
Method 1: Enter the IP address of the network camera as the WAN IP in VioStor.
Method 2: Configure the router to allow internal access to the public IP address and the mapped ports of the network cameras.

3. Recording is not working properly.

A. Make sure the hard disk tray is correctly locked in VioStor.

B. When only one hard disk is installed, make sure the disk is installed in the tray of hard disk 1. Hard disk 1 should be installed on top of hard disk 2.

C. Check if the recording function is enabled in Camera Configuration page (the function is enabled by default). Make sure the IP address, name, and password are correct.

D. If the above items are verified to work properly while the status LED blinks in green, the hard disk(s) may be damaged or cannot be detected.

Please turn off the server and install a new hard disk.

Note: If you have updated the configurations of VioStor, recording will be stopped temporarily and restart again shortly.

4. I cannot login the administration page.

Please check if you have the administrator authority. Only administrators are allowed to login VioStor.

5. The live video is not clear or smooth sometimes.

A. The image quality may be restricted and interfered by the actual network traffic.

B. When there are multiple accesses to the camera or the VioStor server, the image quality will be reduced. And it is recommended to have three simultaneous connections to the monitoring page at maximum. For better recording performance, please do not open too many IE browsers to view the live video.

C. The same camera may be shared by multiple VioStor servers for recording at the same time. Please use dedicated cameras.

6. The alarm recording does not function.

A. Please login the administration page and go to Camera Settings-Alarm Settings. Make sure alarm recording is enabled for the camera.

B. When using Panasonic BB-HCM311 cameras, the camera firmware must be upgraded to v1.3 for alarm recording to work properly.

C. If VioStor is installed behind a router while the network camera is not, alarm recording will not work.

D. When alarm recording is enabled, make sure you have configured the number of days that alarm recordings will be retained in Camera Settings-Advanced Settings. Otherwise, the recordings may be overwritten.

7. The estimated storage space for recording displayed in Recording Settings page is different from the actual value.

This estimated value is for reference only. The actual disk space may vary according to the image contents, network environment, and the performance of the cameras.

8. **The screen is displayed abnormally with strange horizontal lines when the resolution of Panasonic BB-HCM381 camera is set as 640x480.**
   This is due to the interlaced scanning design of the camera. Please login the camera's configuration page and go to Setup->Camera->Vertical Resolution. Then configure the setting as 240.

9. **The E-map cannot be displayed correctly.**
   Please check the file format. VioStor supports E-map in JPEG only.

10. **I cannot find my VioStor in QNAP Finder.**
    A. Check if VioStor is turned on.
    B. Check the network connection of the computer and VioStor.
    C. Refresh QNAP Finder and check the IP address of VioStor. Make sure you have turned off all firewall software on your computer.

11. **The changes to the system configurations cannot take effect.**
    After changing the settings in administration page, click the Apply button to apply the changes.

12. **The monitoring page cannot be fully displayed in Internet Explorer.**
    If you are using the zooming function of Internet Explorer 7, the page may not be displayed properly. Please click F5 to refresh the page.

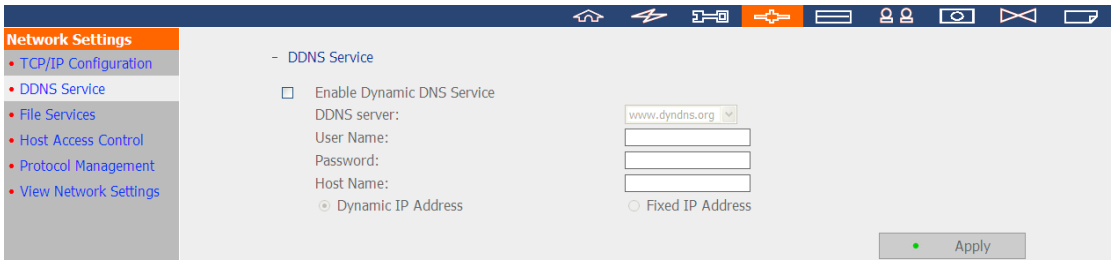
13. **I cannot use the SMB, FTP, and Web File Manager of VioStor.**
    A. Please go to "Network Settings-File Services" page and check if these three functions are enabled.
    B. When VioStor is installed behind a router and the access to VioStor is outside the router, you will not be able to use SMB and FTP services. Please refer to Appendix B for details.

14. **The server takes too long to restart.**
    When the server has been restarting for more than 5 minutes, please turn off the power and turn on the server again. If the problem persists, please contact the technical support.

Appendix A Dynamic Domain Name Registration

The VioStor supports DDNS service provided by DynDNS. You can go to DynDNS website http://www.dyndns.org/ to register a dynamic domain name.

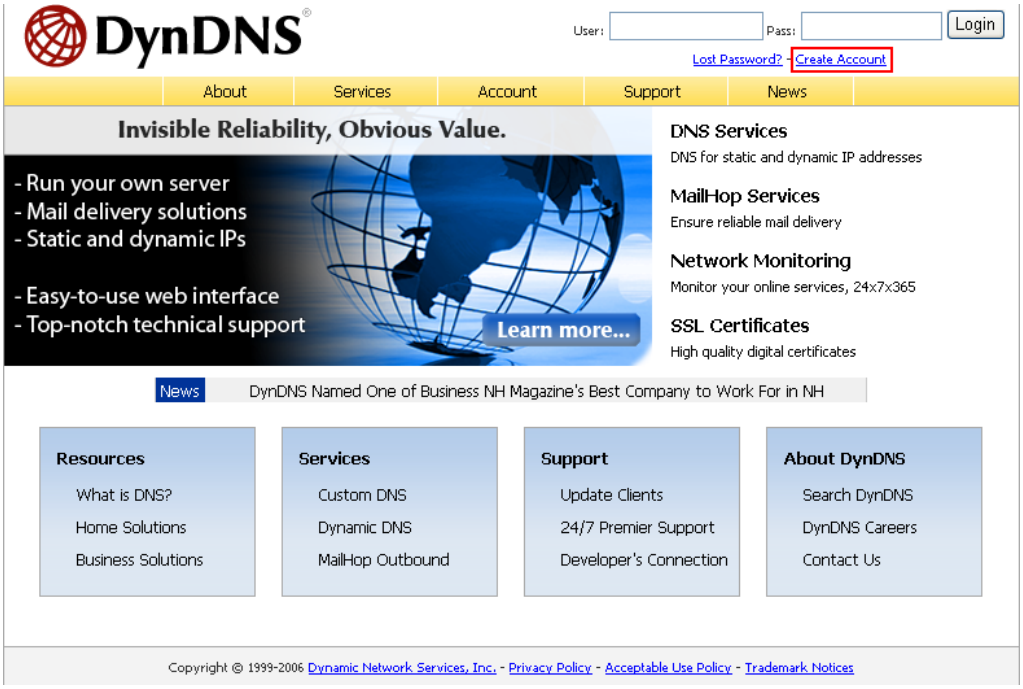
Configure and activate DDNS service to enable the Internet users to access your VioStor via this dynamic domain name. When the ISP assigns a new WAN IP address, the VioStor will update the new address to the DynDNS server automatically.



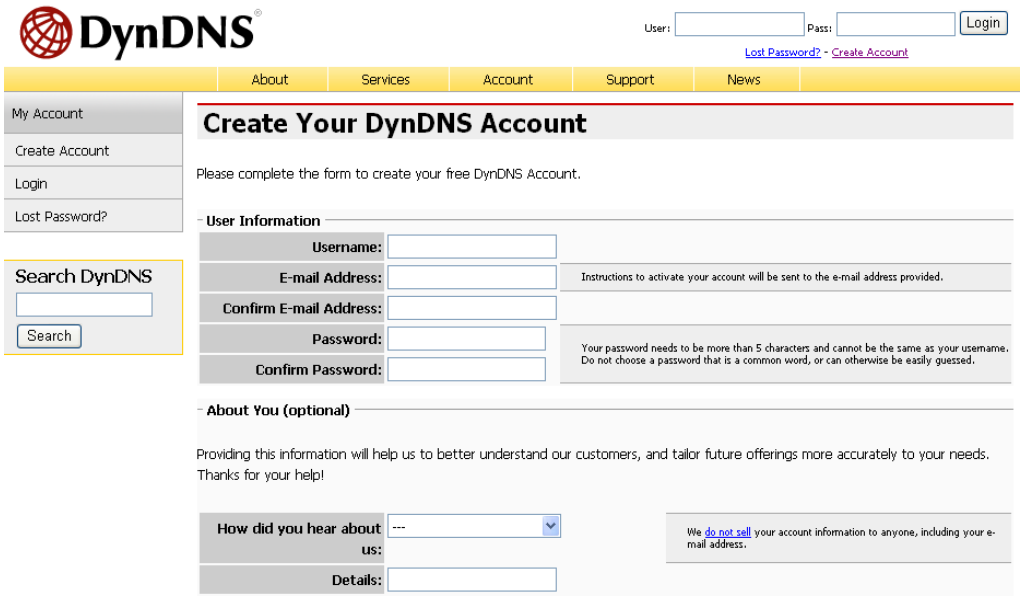
Registration Procedure

Please follow the steps below to register a dynamic domain name. This guide is for reference only. If there are any changes, please refer to the instructions or documents on the web site.

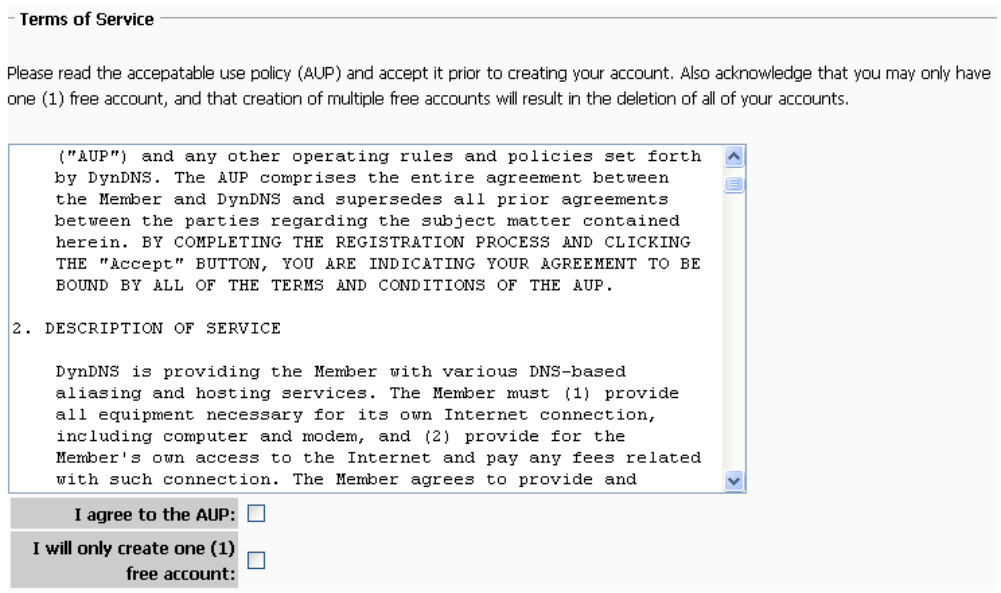
1. Open the browser and connect to http://www.dyndns.com/. Click "Create Account" to begin registration.



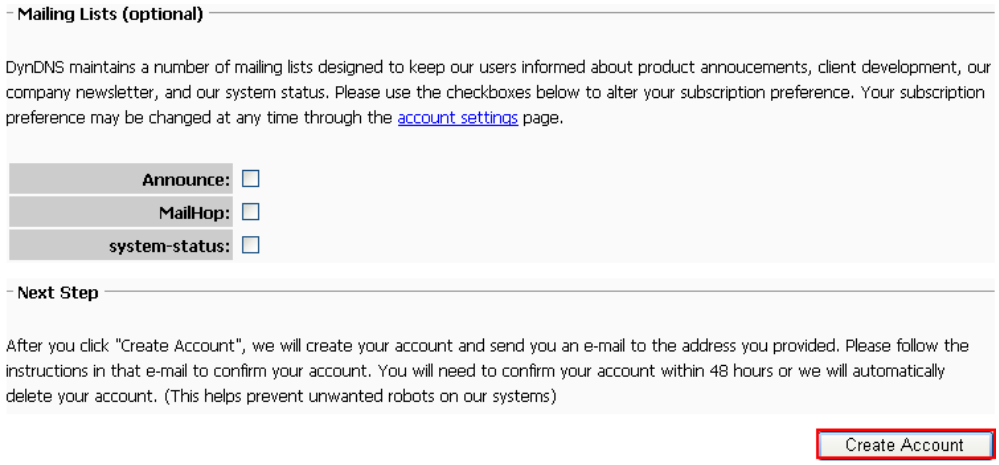
2. Enter the user name, email address, and password to create an account for DDNS service. Please verify your email address to receive the confirmation message from the server.



3. Select to accept the terms of service.



4. Configure the mailing lists if necessary. Then click "Create Account".



5. When your account is successfully created, a confirmation message will be sent to your e-mail address. Please follow the instructions in the e-mail to activate your account within 48 hours. When you have finished the confirmation process, you can apply for your own dynamic domain name. Please refer to the website of the DDNS provider for more information.

Appendix B Configuration Examples

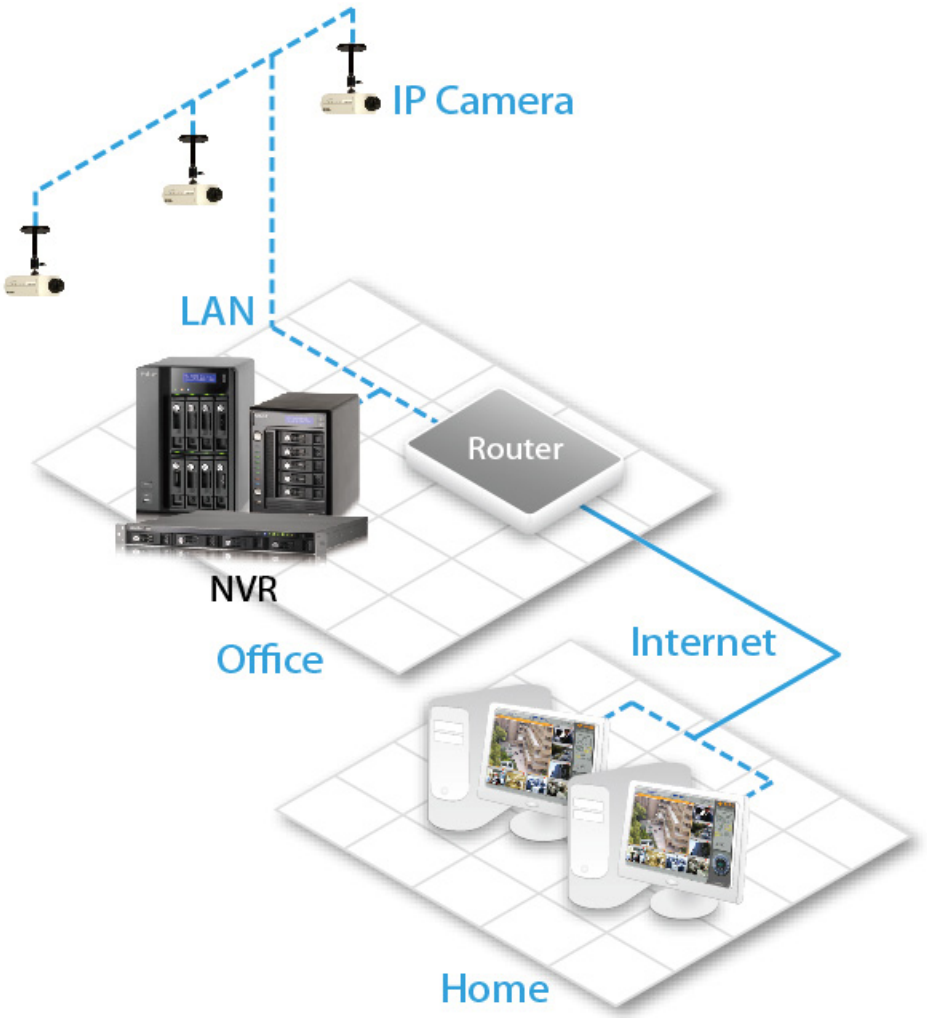
Environment 1: VioStor, IP Camera, and monitoring PC are all in the same network

Network Surveillance Installation for SOHO and SMB

	IP Address
VioStor	*192.168.1.1*
PC	*192.168.1.100*
Camera 1	*192.168.1.101*
Camera 2	*192.168.1.102*
Camera 3	*192.168.1.103*

In the example, just add the camera to the VioStor by entering the cameras' IP address.

Environment 2: The VioStor and the IP camera are installed behind the router, while the monitoring PC is located remotely



	IP Address	Mapped port in router
VioStor	*192.168.1.1*	*8000*
Camera 1	*192.168.1.101*	*8001*
Camera 2	*192.168.1.102*	*8002*
Camera 3	*192.168.1.103*	*8003*
Router public IP	*219.87.144.205*	
PC	*10.8.10.100*	

In this example, to allow a remote PC to connect to the VioStor and the cameras, you need to:

Step 1. Set up port mapping (virtual server) on the router.

From	Forward to
219.87.144.205:8000	*192.168.1.1:80*
219.87.144.205:8001	*192.168.1.101:80*
219.87.144.205:8002	*192.168.1.102:80*
219.87.144.205:8003	*192.168.1.103:80*

Step 2. Add camera to the VioStor by entering the IP address of the camera in the "IP Address" settings, and the public IP address of the router and the mapped ports of the camera to the "WAN IP Address" settings.

Note: When configuring the network camera, WAN IP and LAN IP must be entered.

To open FTP (port 21) and SMB (port 445) of the VioStor on WAN, you have to set the following port mapping settings:

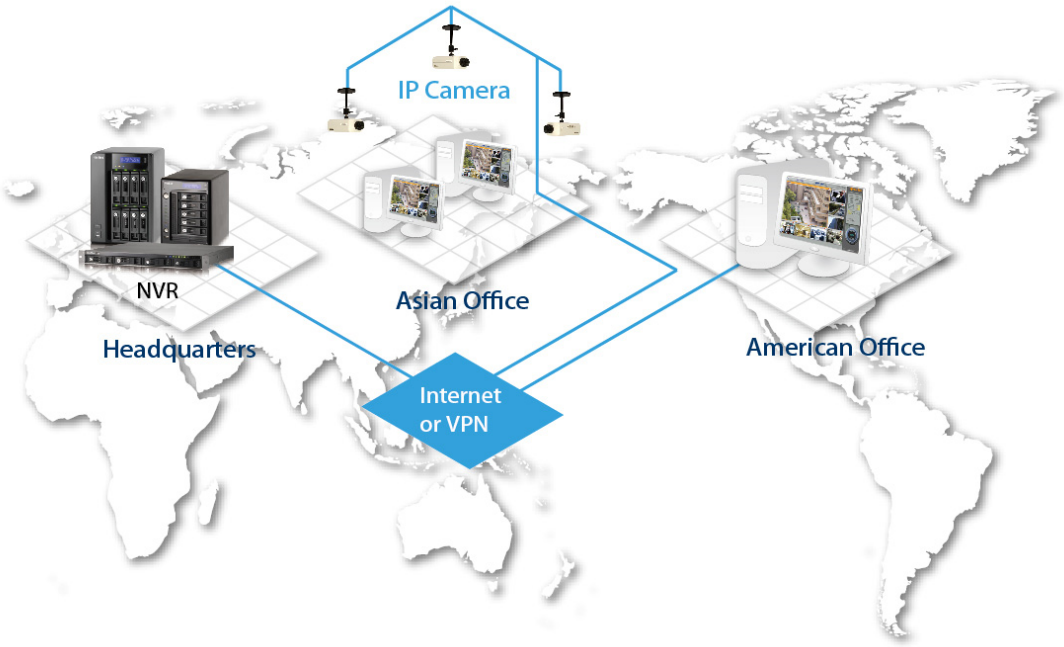
From	Forward to
219.87.144.205:21	*192.168.1.1:21*
219.87.144.205:139	*192.168.1.1:139*
219.87.144.205:445	*192.168.1.1:445*

After finishing the above two steps, you can access the VioStor via WAN by entering the IP address http://219.87.144.205:8000 in the IE browser. Then login the VioStor via the correct user name and password.

If the port specified to the VioStor is 80, you can enter http://219.87.144.205 to access the VioStor as the default port of HTTP is 80.

Note: If the router does not use a fixed IP, you will need to configure DDNS on the router. Other configurations are the same as above.

Environment 3: The VioStor and the IP camera are all located remotely



	IP Address
VioStor	*219.87.144.205*
Camera 1	*61.62.100.101*
Camera 2	*61.62.100.102*
Camera 3	*61.62.100.103*

In this example, just add the camera to the VioStor by adding its IP address to the "IP Address" settings.

Note: If there is a particular port for connecting the camera, please specify the port in the system configuration.

Environment 4: The VioStor and the IP camera are installed behind the router

	IP Address
VioStor 1	192.168.1.101
VioStor 2	192.168.1.102
VioStor 3	192.168.1.103
Router public IP	219.87.145.205

In the example, to allow a PC which is located remotely to access each VioStor via FTP, you need to:

Step 1. Set up port mapping (virtual server) on the router

	From	**Forward to**
VioStor 1	219.87.145.205:2001	192.168.1.101:21
VioStor 2	219.87.145.205:2002	192.168.1.102:21
VioStor 3	219.87.145.205:2003	192.168.1.103:21

You could directly connect VioStor 1 via FTP by ftp://219.87.145.205:2001
You could directly connect VioStor 2 via FTP by ftp://219.87.145.205:2002
You could directly connect VioStor 3 via FTP by ftp://219.87.145.205:2003

Step 2. Enable FTP Port Mapping on the VioStor
If you want to connect each VioStor via FTP by clicking "FTP" in playback page of each VioStor, you need to enable FTP port mapping in "Network Settings" > "File Services" on the system administration page and set the mapped port number.

	Mapped Port
VioStor 1	2001
VioStor 2	2002
VioStor 3	2003

After finishing the above two steps, you can access the VioStor via FTP by entering the IP address in the IE browser or clicking "FTP" in the playback page. Then login the VioStor via the correct user name and password.

Technical Support

QNAP provides dedicated online support and customer service via instant messenger. You can contact us by the following means:

Online Support: http://www.qnapsecurity.com/
MSN: q.support@hotmail.com
Skype: qnapskype

Technical Support in the USA and Canada:
Email: q_supportus@qnap.com
TEL: 909-595-2819 ext. 110
Address: 168 University Parkway Pomona, CA 91768-4300
Service Hours: 08:00-17:00 (GMT- 08:00 Pacific Time, Monday to Friday)

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS
0. Definitions.
“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.
The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of

the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.
All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on

terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.
No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.
You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.
You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
b) The work must carry prominent notices stating that it is released under this

License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.
c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.
d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.
A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.
You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.
b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.
c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and

noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.
d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.
e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.
A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

“Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.
“Additional permissions” are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material)

supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.
All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.
You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent

licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.
You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.
Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives

whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.
A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge

and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.
If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy

simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.
Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.
The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.
THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE

COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.
IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.
If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS